Hillstone Networks

StoneOS WebUI Guide - A series

Version 5.5R11



Copyright 2024 Hillstone Networks. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Hillstone Networks.

Hillstone Networks

Commercial use of the document is forbidden.

Contact Information:

US Headquarters:

Hillstone Networks

5201 Great America Pkwy, #420

Santa Clara, CA 95054

Phone: 1-408-508-6750

https://www.hillstonenet.com/about-us/contact/

About this Guide:

This guide gives you comprehensive configuration instructions of Hillstone Networks StoneOS .

For more information, refer to the documentation site: https://docs.hillstonenet.com

To provide feedback on the documentation, please write to us at: TechDocs@hillstonenet.com

Hillstone Networks

TWNO: TW-WUG-UNI-A-5.5R11-EN-V1.0-2024-09-12

Contents

Contents 1

Welcome 1

Conventions 2

Explorer Compatibility 9

Chapter 1 Getting Started Guide 10

Log in to WebUI 12

Startup Wizard 13

Skipping the Startup Wizard 14

Starting the Startup Wizard 14

Preparing the StoneOS System 21

Configuring the System Time 22

Configuring the System Time Manually 22

Configuring NTP 23

Installing Licenses 25

Creating a System Administrator 25

Adding Trusted Hosts 28

Upgrading StoneOS Firmware 31

Configuring a DNS Server 32

Updating Signature Database 32

Connecting to the Internet 33

Connecting to the Internet Under Routing Mode 33
Connecting to the Internet Under Transparent Mode 40
Connecting to the Internet via mobile 3G/4G 48
Restoring Factory Settings 53
Restoring via the CLR Button 53
Restoring via WebUI 55
General Features 55
Device Management 57
Configuring Password Policies 57
Application Scenario 57
Configuration Steps: 58
Backing up and Restoring System Configuration 62
Application Scenario 62
Configuration Steps 62
Exporting System Debug Information 65
Application Scenario 65
Configuration Steps: 65
Threat Prevention 66
Application Scenario 67
Configuration Steps 67
High Availability (HA) 79
Requirements 79

Application Scenario 80
Configuration Steps 81
Exporting Logs 93
Application Scenario 93
Configuration Steps 93
Chapter 2 Deploying Your Device 99
How a Firewall Works 100
StoneOS System Architecture 100
General Rules of Security Policy 102
Packet Processing Rule 104
Forwarding Rule in Layer 2 104
Forwarding Rule in Layer 3 106
Deploying Transparent Mode 109
Deploying Routing Mode 119
Deploying Mix Mode 128
Deploying Tap Mode 129
Chapter 3 Dashboard 132
Customization 132
Threats 132
Threatscape 133
User 133
Application 134

Total Traffic 134
Physical Interface 134
System and Signature Database 135
System Information 135
Signature DB Information 136
License 137
Specified Period 137
Chapter 4 iCenter 139
Threat 139
Hot Threat Intelligence 145
Viewing Hot Threat Intelligence 149
Chapter 5 Network 151
Security Zone 152
Configuring a Security Zone 153
Interface 156
Configuring an Interface 158
Creating a PPPoE Interface 158
Creating a Tunnel Interface 176
Creating a Virtual Forward Interface 189
Creating a Loopback Interface 194
Creating an Aggregate Interface 198
Creating a Redundant Interface 209

Creating an Ethernet Sub-interface/an Aggregate Sub-interface/a Redundant Sub-interface 210
Creating a VSwitch Interface 218
Creating a Vif Interface 219
Editing an Interface 224
Viewing the Interface Status 238
Interface Group 239
Creating an Interface Group 240
LLDP 240
LLDP Work Mode 241
Configuring LLDP 241
Enabling LLDP 242
Modifying LLDP Configuration 244
Viewing MIB Topology 246
Management Interface 248
Configuring a Management Interface 248
DNS 253
Configuring a DNS Server 253
Configuring a DNS Proxy 254
Configuring a DNS Proxy Rule 254
Enabling/Disabling a DNS Proxy Rule 261
Adjusting DNS Proxy Rule Position 261

DNS Proxy Global Configuration 262
DNS Proxy Hit Analysis 263
Configuring an Analysis 264
Configuring a DNS Cache 265
Configuring Host TTL 267
NBT Cache 269
DHCP 270
Configuring a DHCP Server 270
Configuring a DHCP Relay Proxy 280
Configuring a DHCPv6 Server 281
Configuring a DHCPv6 Relay Proxy 284
DDNS 284
Configuring a DDNS 285
PPPoE 288
Configuring PPPoE 289
Virtual Wire 291
Configuring a Virtual-Wire 292
Configuring the Virtual Wire Mode 293
Virtual Router 294
Creating a Virtual Router 295
Global Configuration 295
Virtual Switch 296

Creating a VSwitch 296
Port Mirroring 298
Limits and Precautions 298
WLAN 302
Creating a WLAN 302
Advanced Settings 305
3G/4G 307
Configuring 3G/4G Settings 307
Managing Data Card 310
4G Module Password Authentication 310
Automatically Verifying the PIN Code 311
Enabling/Disabling the PIN Code Protection 311
Modifying the PIN Code 312
Manually Verifying the PIN Code 312
Unlocking the PIN Code 313
Load Balancing 313
SLB 313
LLB 314
Outbound Link Load Balancing 315
Outbound Load Balancing Implementation Mechanism 315
Configuration Method 315
Configuring Outbound Link Load Balancing 317

Configuring SLA Profile 317
Configuring LLB Profile 329
Configuring LLB Rule 333
Inbound Link Load Balancing 337
Configuring Inbound Link Load Balancing 337
Creating a Smart DNS Rule Table 337
Application Layer Gateway (ALG) 339
Enabling ALG 340
Enabling/Disabling DNS Rewrite by DNAT 342
Global Network Parameters 342
Configuring Global Network Parameters 342
Configuring Protection Mode 348
IPv6 Tunnel 349
IPv6 over IPv4 Tunnel 349
Configuring an Automatic 6to4 Tunnel 350
Configuring a Manual 6to4 Tunnel 351
Configuring an ISATAP Tunnel 353
Configuring a 6RD Tunnel 355
Chapter 6 Advanced Routing 359
Destination Route 361
Creating a Destination Route 361
Destination-Interface Route 364

Creating a Destination-Interface Route 364
Source Route 367
Creating a Source Route 367
Source-Interface Route 369
Creating a Source-Interface Route 370
ISP Route 372
Creating an ISP Route 372
ISP Profile 375
Creating an ISP Profile 375
Deleting a User-defined ISP Profile 377
Uploading a User-defined ISP Profile 377
Downloading an ISP Profile 378
Policy-based Route 378
Creating a Policy-based Route 378
Creating a Policy-based Route Rule 380
Adjusting Priority of a PBR Rule 386
Applying a Policy-based Route 387
DNS Redirect 389
Configuring the Global Match Order 389
RIP 390
Creating RIP 390
OSPF 395

OSPF GR 395
Creating OSPF 397
Viewing the Neighbor Information 403
Configuring OSPFv3 404
Creating OSPFv3 405
Viewing Neighbor Information 417
Configuring BGP 418
BGP GR 418
Basic 421
Neighbor List 430
Delete BGP 431
Route Object 431
Route Map 431
Configuring a Route Map 435
Access List Route 440
Configuring an Access List Route 441
AS Path Access List 444
Configuring an AS Path Access List 445
Community List 446
Configuring a Community List 447
Configuring Protocol Independent Multicast (PIM) 448
Basic Principles of PIM-SM 449

PIM-SSM 450
Configuring PIM 451
Viewing PIM Routing Information 459
Configuring Protocol Independent Multicast (PIMv6) 460
Multicast Listener Discovery (MLD) 460
MLDv1 461
Configuring PIMv6 461
Viewing PIMv6 Routing Information 468
Chapter 7 Authentication 469
Authentication Process 469
Web Authentication 470
Enabling the WebAuth 471
Configuring Basic Parameters for WebAuth 471
Customizing WebAuth Page 482
NTLM Authentication 484
Step 1: Configure NTLM for System 484
Step 2: Configure settings for User Browser 485
Single Sign-On 485
Enabling SSO Radius for SSO 488
SSO Web for SSO 491
Typical Scenarios of SSO Web for SSO 491
Configuring SSO Web for SSO 492

Configuring SSO Web for SSO 493
Constructing an HTTP(S) RESTful API Request in the Third-Party Authentication System 494
Using AD Scripting for SSO 496
Step 1: Configuring the Script for AD Server 496
Step 2: Configuring AD Scripting for StoneOS 499
Radius Snooping 501
Realizing SSO via Agile Controller 502
Using AD Polling for SSO 506
Using SSO Monitor for SSO 511
Configuration Examples of Using SSO Monitor for SSO 515
Step 1: Installing and Running AD Security Agent on a PC or Server 516
Step 2: Configuring AD server for StoneOS 520
Step 3: Enabling and Configuring SSO Monitor 521
Using TS Agent for SSO 522
Step 1: Installing and running Hillstone Terminal Service Agent in Windows server 522
Step 2: Configuring TS Agent parameters in StoneOS 533
802.1x 536
Configuring 802.1x 537
Creating 802.1x Profile 537
802.1x Global Configuration 540
Viewing Online Users 542

PKI 542
Creating a PKI Key 544
Creating a Trust Domain 546
Importing/Exporting Trust Domain 550
Importing Trust Certification 551
Configuring a Certificate Chain 551
Creating a Certificate Chain 551
Exporting a Certificate Chain 553
Configuring Certificate Validity Check 553
Online Users 554
Chapter 8 VPN 555
IPSec VPN 556
Basic Concepts 556
Security Association (SA) 556
Encapsulation Modes 556
Establishing SA 557
Using IPSec VPN 557
Configuring an IPSec VPN 558
Configuring an IPSec VPN 558
Configuring a VPN Peer 566
Editing a VPN Peer 572
Deleting a VPN Peer 573

Copying a VPN Peer 573
Configuring a Phase 1 Proposal 573
Configuring a Phase 2 Proposal 578
Configuring the Smart Link 583
Editing an IPSec VPN 586
Deleting an IPSec VPN 586
Enabling or Disabling an IPSec VPN 587
Copying an IPSec VPN 588
Viewing IPSec VPN Entry 588
Configuring a Manual Key VPN 589
Deleting a Manual Key VPN 592
Viewing Manual Key VPN Entry 593
Viewing IPSec VPN Monitoring Information 593
Configuring PnPVPN 597
PnPVPN Workflow 598
PnPVPN Link Redundancy 599
Configuring a PnPVPN Client 599
Configuring IPSec-XAUTH Address Pool 601
SSL VPN 605
Configuring an SSL VPN 606
Configuring Resource List 626
Host Binding 628

Configuring Host Binding 629
Configuring Host Binding and Unbinding 629
Configuring a Super User 630
Configuring a Shared Host 631
Importing/Exporting Host Binding List 632
Host Compliance Check 633
Role Based Access Control and Host Compliance Check Procedure 634
Configuring a Host Compliance Check Profile 635
Secure Connect Client Management 641
Secure Connect Client Management Configuration 642
Customizing Secure Connect Download Page 642
Customizing Client Download Source 643
Hillstone Secure Connect Client for Windows 644
Downloading and Installing the Client 645
Starting Up and Connecting 645
Editing and Deleting Login Entry 655
Viewing Connection and Statistics Information 656
Viewing Interface and Routing Information 657
Viewing Log Information 658
Configuring Check for Updates 659
Third-party USB Key 659
Client Menu 660

General Configuration 661
Uninstalling the Client 662
Hillstone Secure Connect Client for Android 662
Downloading and Installing the Client 662
Starting Up and Connecting 663
Editing and Deleting Login Entry 668
Viewing Connection Information 668
Hillstone Secure Connect Client for iOS 669
Downloading and Installing the Client 670
Starting Up and Connecting 670
Editing and Deleting Login Entry 674
Viewing Connection Information 674
Hillstone Secure Connect Client for macOS 675
Downloading and Installing the Client 676
Starting Up and Connecting 676
Editing and Deleting Login Entry 680
Viewing Connection and Statistics Information 681
Viewing Interface and Routing Information 682
Viewing Log Information 683
Configuring Check for Updates 684
Client Menu 684
General Configuration 685

Uninstalling the Client 686
Hillstone Secure Connect Client for Linux 686
Downloading and Installing the Client 687
Starting Up and Connecting 687
Editing and Deleting Login Entry 691
Viewing Connection and Statistics Information 692
Viewing Interface and Routing Information 693
Viewing Log Information 694
Configuring Check for Updates 695
Client Menu 695
General Configuration 696
Hillstone Secure Connect Client for ChineseOS 697
Downloading and Installing the Client 698
Starting Up and Connecting 698
Editing and Deleting Login Entry 705
Viewing Connection and Statistics Information 705
Viewing Interface and Routing Information 706
Viewing Log Information 707
Configuring Check for Updates 708
General Configuration 708
General Configuration 709
Client Menu 710

Uninstalling the Client 711
L2TP VPN 711
Configuring a LNS 711
Configuring an L2TP VPN 711
Configuring an L2TP VPN Address Pool 716
Viewing L2TP VPN Online Users 719
Configuring Device as L2TP Client 719
Configuring a L2TP Client 719
VXLAN 722
Creating VXLAN Static Tunnel 722
GRE VPN 723
Configuring GRE VPN 724
Chapter 9 Zero Trust Network Access (ZTNA) 727
Introduction 727
ZTNA Typical Scenarios 729
Remote Access 729
Intranet Access 730
Configuring ZTNA Gateway 731
Configuring ZTNA Remote Access 732
Configuring ZTNA Intranet Access 748
Managing Endpoint Items 761
Introduction 761

Windows Endpoint Item Management 762
macOS Endpoint Item Management 767
Linux Endpoint Item Management 771
ChineseOS Endpoint Item Management 774
iOS Endpoint Item Management 777
Android Endpoint Item Management 780
Endpoint Tags 782
Introduction 782
Configuring an Endpoint Tag 783
Application Resource/Application Resource Group 785
Introduction 785
Configuring an Application Resource/Application Resource Group 785
ZTNA Policy 790
Description about ZTNA Policy Matching 791
Configuring ZTNA Policy 792
Address Pool 798
Introduction 798
Configuring an Address Pool 798
Single Packet Authorization (SPA) 801
Introduction 801
Configuring Single Packet Authorization (SPA) 801
Secure Connect Client Management 803

Customizing Secure Connect Download Page 803
Customizing Client Download Source 804
ZTNA Portal 805
Monitor 806
ZTNA License Usage 806
Online Endpoint Statistics 807
Endpoint Hit Top 10 808
User Traffic Top 10 808
Viewing and Managing Online Users 809
Endpoint Tag Log 810
Chapter 10 Object 813
Address 814
Global Configuration of Address Book 815
Enabling Ordered Address Book Function 815
Creating an Address Book 816
Exporting User-defined Address Books 824
Importing User-defined Address Books 825
Viewing Details 825
Searching Address Entries 826
Device Object 828
Configuring a Device Object 829
Creating a Device Object 829

Editing a Device Object 830
Deleting a Device Object 831
Viewing the Mapping IP Details of Device 831
Host Book 831
Creating a Host Book 832
Editing a Host Book 833
Deleting a Host Book 833
Viewing Details 834
Custom IP Geolocation 835
Creating a Custom IP Geolocation 835
Editing a Custom IP Geolocation 836
Deleting a Custom IP Geolocation 837
Querying Geolocation 837
Filtering Custom IP Geolocation Entries 837
Service Book 838
Predefined Service/Service Group 838
User-defined Service 838
User-defined Service Group 839
Configuring a Service Book 839
Configuring a User-defined Service 839
Exporting User-defined Services 844
Importing User-defined Services 845

Configuring a User-defined Service Group 846
Exporting User-defined Service Groups 847
Importing User-defined Service Groups 847
Viewing Details 848
Searching Service Entries 848
Searching Service Groups 850
Application Book 851
Editing a Predefined Application 851
Creating a User-defined Application 852
Exporting User-defined Applications 854
Importing User-defined Applications 855
Creating a User-defined Application Group 855
Exporting User-defined Application Groups 856
Importing User-defined Application Groups 857
Creating an Application Filter Group 858
Creating a Signature Rule 859
Viewing Details 867
Application Resource/Application Resource Group 867
Introduction 867
Configuring an Application Resource/Application Resource Group 867
Configuring an Address Pool 871
SSL Proxy 875

Work Mode 875
Working as the Gateway of Web Clients 877
Configuring SSL Proxy Parameters 877
Specifying the PKI Trust Domain of Device Certificate 878
Obtaining the CN Value 878
Importing Device Certificate to Client Browser 879
Configuring an SSL Proxy Profile 880
Binding an SSL Proxy Profile to a Policy Rule 891
Working as the Gateway of Web Servers 891
Configuring an SSL Proxy Profile 891
Binding an SSL Proxy Profile to a Policy Rule 897
Configuring Domain White List 898
Creating a User-defined Domain White List 898
Editing a User-defined Domain White List 899
Deleting a User-defined Domain White List 899
Exporting the Domain White List 900
Configuring the IP Whitelist 901
Configuring Dynamic IP Whitelist 901
Configuring the Validity Time of the Dynamic IP Whitelist 901
Configuring the Dynamic IPs on the Whitelist to be Permanently Valid 902
Configuring Static IP Whitelist 902
Deleting IP Whitelist 903

SLB Server Pool 904
Configuring SLB Server Pool and Track Rule 904
Viewing Details of SLB Pool Entries 908
Schedule 910
Periodic Schedule 910
Absolute Schedule 910
Creating a Schedule 910
AAA Server 912
Configuring a Local AAA Server 913
Configuring Radius Server 923
Configuring Active Directory Server 929
Configuring LDAP Server 938
Configuring TACACS+ Server 944
Configuring an OAuth2 Server 946
Connectivity Test 952
Radius Dynamic Authorization 953
User 955
Configuring a Local User 955
Creating a Local User 956
Creating a User Group 960
Export User List 960
Import User List 961

Configuring a LDAP User 962
Creating a LDAP User 962
Configuring Account Expiration 963
Exporting User List 964
Importing User List 964
Synchronizing Users 966
Configuring an Active Directory User 966
Creating an Active Directory User 966
Configuring Account Expiration 967
Exporting User List 968
Importing User List 968
Synchronizing Users 970
Configuring a IP-User Binding 970
Adding User Binding 970
Import Binding 972
Export Binding 972
User Going Offline Alarm 972
Creating a User Going Offline Alarm Profile 973
Role 976
Configuring a Role 977
Creating a Role 977
Mapping to a Role Mapping Rule 978

Creating a Role Mapping Rule 979
Configuring a User Attribute Instance 980
Creating a Role Combination 983
Creating a Role Blacklist 984
Track Object 985
Creating a Track Object 985
Track Object List 990
URL Filtering 992
Configuring URL Filtering 992
Cloning a URL filtering Rule 1000
Viewing URL Hit Statistics 1000
Viewing Web Surfing Records 1001
Configuring URL Filtering Objects 1001
Predefined URL DB 1002
Configuring Predefined URL Database Update Parameters 1002
Upgrading Predefined URL Database Online 1002
Upgrading Predefined URL Database from Local 1003
User-defined URL DB 1003
Configuring User-defined URL DB 1003
Importing User-defined URL 1004
Clearing User-defined URL 1005
URL Lookup 1005

Inquiring URL Information 1005
Configuring URL Lookup Servers 1006
Keyword Category 1007
Configuring a Keyword Category 1008
Warning Page 1009
Enabling/ Disabling the Block Warning 1010
Enabling/ Disabling the Audit Warning 1011
First Access of Uncategorized URL 1012
Configuring the URL Blacklist/Whitelist 1013
Configuring the URL Blacklist 1014
Configuring the URL Whitelist 1016
Data Security 1018
Configuring Objects 1019
Predefined URL DB 1020
Configuring Predefined URL Database Update Parameters 1020
Upgrading Predefined URL Database Online 1021
Upgrading Predefined URL Database from Local 1021
User-defined URL DB 1021
Configuring User-defined URL DB 1021
Importing User-defined URL 1022
Clearing User-defined URL 1023
URL Lookup 1023

Inquiring URL Information 1023
Configuring URL Lookup Servers 1024
Keyword Category 1025
Configuring a Keyword Category 1026
Warning Page 1027
Enabling/ Disabling the Block Warning 1028
Enabling/ Disabling the Audit Warning 1029
Bypass Domain 1030
Exempt User 1031
File Filter 1033
Creating File Filter Rule 1033
Viewing File Filter Logs 1036
Content Filter 1036
File Content Filter 1037
Configuring File Content Filter 1037
Viewing Monitored Results of Keyword Blocking in File Content 1040
Viewing Logs of Keyword Blocking in File Content 1041
Web Content 1042
Configuring Web Content 1042
Viewing Monitored Results of Keyword Blocking in Web Content 1047
Viewing Logs of Keyword Blocking in Web Content 1047
Web Posting 1048

Configuring Web Posting 1048
Viewing Monitored Results of Keyword Blocking in Web Posts 1053
Viewing Logs of Keyword Blocking in Web Posts 1053
Email Filter 1054
Configuring Email Filter 1054
Viewing Monitored Results of Email Keyword Blocking 1058
Viewing Logs of Emails Keyword Blocking 1058
APP Behavior Control 1059
Configuring APP Behavior Control 1059
Viewing Logs of APP Behavior Control 1065
Network Behavior Record 1066
Configuring Network Behavior Recording 1066
Viewing Logs of Network Behavior Recording 1070
End Point Protection 1070
Configuring End Point Protection 1071
Preparing 1071
Configuring End Point Protection Function 1071
Configuring End Point Protection Rule 1072
Configuring End Point Security Control Center Parameters 1075
ACL 1077
ACL Profile 1077
Honeypot 1081

Introduction 1081
Configuring the Honeypot Function 1082
Connecting to Honeypot 1082
Configuring a Trap Rule 1084
Viewing and Handling the Threat Information about Attackers 1086
Chapter 11 Policy 1088
Security Policy 1089
Configuring a Security Policy Rule 1090
Managing Security Policy Rules 1113
Enabling/Disabling a Policy Rule 1113
Cloning a Policy Rule 1114
Adjusting Security Policy Rule Position 1114
Configuring Default Action 1114
Filtering Policy Rules by Using Custom Policy Rule Attributes 1116
Policy Global Configuration 1118
Switching between Multi-zone and Single-zone 1119
Security Policy Matching Destination Addresses After DNAT 1119
Enabling/Disabling Traffic Statistics of Policies 1120
Enabling/Disabling the Delay Address Update Time Function 1120
Enabling Traffic Statistics of Policy Assistant 1121
Schedule Validity Check 1121
Showing Disabled Policies 1122

Importing Policy Rule 1123
Exporting Policy Rule 1124
Searching Policy Rule 1126
Configuring Policy Audit Function 1129
Enabling the Configuration Audit Function 1129
Adding the Audit Comment 1130
Viewing audit history 1131
Enabling Traffic Statistics of Policy Assistant 1132
Configuring an Aggregate Policy 1133
Creating an Aggregate Policy 1133
Adding an Aggregate Policy Member 1134
Removing an Aggregate Policy Member 1136
Deleting an Aggregate Policy 1137
Adjusting Position of an Aggregate Policy 1138
Enabling/Disabling an Aggregate Policy 1140
Configuring a Policy Group 1141
Creating a Policy Group 1141
Deleting a Policy Group 1143
Enabling/Disabling a Policy Group 1143
Adding/Deleting a Policy Rule Member 1143
Editing a Policy Group 1144
Showing Disabled Policy Group 1144

Mini Policy 1145
Configuring a Mini Policy 1145
Creating a Mini Policy 1146
Deleting a Mini Policy 1148
Editing a Mini Policy 1148
Enabling/Disabling a Mini Policy 1149
Viewing and Searching Security Policy Rules/ Policy Groups/ Mini Policy 1149
Viewing the Policy/ Policy Group/ Mini Policy 1149
Searching Security Policy Rules/ Policy Groups/ Mini Policy 1151
Policy Optimization 1154
Policy Hit Analysis 1154
Rule Redundancy Check 1157
Performing Redundancy Check on Policy Rules 1158
Configuring Ignored Time of Redundant Policy Rules 1160
Managing the Ignored List 1161
Configuring the Policy Assistant 1162
Enabling the Policy Assistant 1162
Displaying Traffic 1163
Replacing Policy 1166
Application Scenario Example 1167
Configuring Replacement Conditions 1167
Aggregating Policy 1169

Generating Address book 1172
Generating Service Book 1174
Generating Policy 1175
User Online Notification 1177
Configuring User Online Notification 1177
Configuring the Parameters of User Online Notification 1178
Viewing Online Users 1179
NAT 1180
Basic Translation Process of NAT 1180
Implementing NAT 1181
Configuring SNAT 1182
Enabling/Disabling a SNAT rule 1191
Viewing and Searching SNAT Rules 1192
Adjusting Priority 1193
Copying/Pasting a SNAT rule 1194
Importing SNAT rule 1194
Exporting SNAT rule 1195
Exporting NAT444 Static Mapping Entries 1197
Configuring SNAT Optimization 1197
Hit Count 1197
Clearing NAT Hit Count 1198
Hit Count Check 1198

Redundancy Check 1198
Configuring DNAT 1200
Configuring an IP Mapping Rule 1200
Configuring a Port Mapping Rule 1202
Configuring an Advanced NAT Rule 1205
Enabling/Disabling a DNAT Rule 1212
Viewing and Searching DNAT Rules 1212
Copying/Pasting a DNAT Rule 1214
Adjusting Priority 1214
Importing DNAT rule 1215
Exporting DNAT rule 1216
Configuring DNAT Optimization 1218
Hit Count 1218
Clearing NAT Hit Count 1218
Hit Count Check 1219
Redundancy Check 1219
Configuring DNS Rewrite 1220
Configuring a DNS Rewrite Rule 1221
Managing DNS Rewrite Rules 1222
Viewing Dynamic Mapping Table of DNS Rewrite 1223
SLB Server 1224
Viewing SLB Server Status 1224

Viewing SLB Server Pool Status 1224
iQoS 1225
Implement Mechanism 1226
Pipes and Traffic Control Levels 1227
Pipes 1227
Traffic Control Levels 1230
Enabling iQoS 1231
Pipes 1233
Basic Operations 1233
Configuring a Pipe 1234
Searching QoS Policy 1249
Viewing Statistics of Pipe Monitor 1250
Session Limit 1251
Configuring Session Limit 1251
Configuring a Session Limit Rule 1251
Clearing Statistic Information 1254
Traffic Quota 1255
Configuring the Traffic Quota Rule 1256
Configuring the User/ User Group Traffic Quota Rule 1256
Adjusting Traffic Quota Rule Priority 1257
Configuring the Traffic Quota Profile 1258
Configuring the Traffic Quota Zone 1259

Share Access 1260
Configuring Share Access Rules 1260
ARP Defense 1264
Configuring ARP Defense 1266
Configuring Binding Settings 1266
Adding a Static IP-MAC-Port Binding 1266
Obtaining a Dynamic IP-MAC-Port Bindings 1267
Viewing the Timeout Period of ARP Entries and MAC Entries 1269
Bind the IP-MAC-Port Binding Item 1270
Importing/Exporting Binding Information 1270
Configuring ARP Inspection 1271
Configuring DHCP Snooping 1273
Viewing DHCP Snooping List 1276
Configuring Host Defense 1277
Perimeter Traffic Filtering 1279
Configuring IP Blacklist 1280
Static IP Blacklist 1280
Redundancy Check 1282
Blacklist Library Rule 1283
Blacklist Library Details 1284
Dynamic IP Blacklist 1287
Real IP Blacklist 1289

Hit Statics 1290
Service Blacklist 1291
MAC Blacklist 1293
IP Reputation Filtering 1294
Configuring IP Whitelist 1295
Global Search 1296
Configuration 1297
Chapter 12 Threat Prevention 1299
Threat Protection Signature Database 1300
Anti-Virus 1302
Configuring Anti-Virus 1303
Preparing 1303
Configuring Anti-Virus Function 1303
Configuring an Anti-Virus Rule 1305
Cloning an Anti-Virus Rule 1308
Configuring Anti-Virus Whitelist Function 1309
Creating an Anti-Virus Whitelist 1309
Editing an Anti-Virus Whitelist 1310
Deleting an Anti-Virus Whitelist 1310
Configuring Anti-Virus Global Parameters 1310
Enabling / Disabling the Anti-Virus function 1310
Configuring the Decompression Control Function 1312

Intrusion Prevention System 1315
Signatures 1315
Configuring IPS 1317
Preparation 1317
Configuring IPS Function 1317
Configuring an IPS Rule 1320
Cloning an IPS Rule 1367
IPS Global Configuration 1367
Signature List 1369
Searching Signatures 1370
Managing Signatures 1370
Configuring IPS White list 1374
Sandbox 1376
Configuring Sandbox 1377
Preparation 1378
Configuring Sandbox 1378
Configuring a Sandbox Rule 1380
Threat List 1386
Trust List 1386
Sandbox Global Configurations 1387
Attack-Defense 1389
ICMP Flood and UDP Flood 1389

ARP Spoofing 1390
SYN Flood 1390
WinNuke Attack 1390
IP Address Spoofing 1390
ICMP Redirect Attack 1391
IP Address Sweep and Port Scan 1391
Ping of Death Attack 1391
Teardrop Attack 1391
Smurf Attack 1392
Fraggle Attack 1392
Land Attack 1392
IP Fragment Attack 1392
IP Option Attack 1392
Huge ICMP Packet Attack 1393
TCP Flag Attack 1393
DNS Query Flood Attack 1393
DNS Reply Flood Attack 1393
TCP Split Handshake Attack 1393
SIP Flood 1393
Configuring Attack Defense 1394
Configuring Flood Protection Threshold Learning 1416
Configuring Flood Protection Threshold Learning Parameters 1416

Enabling Flood Protection Threshold Learning 1419
Viewing and Applying Flood Protection Threshold Learning Result 1420
Antispam 1422
Configuring Antispam 1422
Preparing 1423
Configuring Antispam Function 1423
Configuring an Antispam Rule 1424
Configuring an Anti-Spam User-defined Blacklist 1427
Antispam Global Configuration 1428
Botnet Prevention 1429
DGA Detection 1429
DNS Tunnel Detection 1430
Configuring Botnet Prevention 1431
Preparing 1431
Configuring Botnet Prevention Function 1431
Configuring a Botnet Prevention Rule 1432
Address Library 1435
Exclude List 1436
Creating a Custom Exclude List 1436
Deleting a Custom Exclude List 1437
Filtering a Entry in the Exclude List 1437
Block List 1437

Creating a Custom Block List 1437
Configuring the Blacklist Library 1439
Cloud Cache 1444
Clearing All Cloud Cached Data 1446
Botnet Prevention Global Configuration 1446
Encrypted Traffic Detection 1448
Configuring the Encrypted Traffic Detection Function 1449
End Point Protection 1452
Configuring End Point Protection 1453
Preparing 1453
Configuring End Point Protection Function 1453
Configuring End Point Protection Rule 1454
Configuring End Point Security Control Center Parameters 1458
End Point Monitor 1459
IoT Monitor 1460
Typical Deployment Scenario 1461
Built-in Asset Identification 1462
External Asset Identification 1462
Configuration Procedure of IoT Monitor Function 1463
Deploying the Asset Identification System on the Virtual Machine 1465
Deploying the Asset Identification System on VMware ESXi 1465
Before You Start 1465

System Requirements and Limits 1466
Procedure 1466
Step 1: Log in to VMware ESXi 1466
Step 2: Create a VM 1466
Step 3: Log in to the virtual machine 1470
Step 4: Configure NIC 1470
Step 5: Install the asset identification program 1471
Deploying the Asset Identification System on Openstack 1472
Before You Start 1472
System Requirements 1472
Procedure 1473
Step 1: Import the Image File 1473
Step 2: Create a Flavor 1474
Step 3: Create a Network 1475
Step 4: Start the Instance 1475
Step 5: Log in to Virtual Machine 1476
Setp 6: Configure NIC 1476
Step 7: Install the asset identification program 1477
Identification List 1479
Configuring the Identification List 1479
Creating Identification List Profile 1480
Importing Identification List 1482

Configuring Region 1483
Creating a Region 1483
Terminal Type 1484
Checking Whether Device is in Repository 1485
Filtering Repository Devices 1485
Configuring IoT Global Configuration 1485
IoT Monitor 1487
Summary 1487
Screening Monitoring Mode 1488
Details 1489
IoT Log 1491
Cloud-Network Collaborative DNS Protection 1493
Unknown Domain Cloud Collaborative Query 1493
Introduction 1493
Typical Application Scenario 1494
Configuring Unknown Domain Cloud Collaborative Query 1494
Enabling Unknown Domain Cloud Collaborative Query 1496
Querying the Cloud Query Results by IP/Domain/URL 1498
Clearing Cloud Query Cached Data 1500
Cloud-Based DNS Security Detection 1500
Introduction 1500
Typical Application Scenario 1500

Configuring Cloud-Based DNS Security Detection 1501
Chapter 13 Monitor 1504
Monitor 1504
User-defined Monitor 1505
Creating a User-defined Stat-set 1515
Viewing User-defined Monitor Statistics 1516
Application Monitor 1517
Summary 1517
Application Details 1519
Group Details 1520
Select Application Group 1521
Statistical Period 1523
Cloud Application Monitor 1523
Summary 1523
Cloud Application Details 1524
Statistical Period 1525
Share Access Monitor 1525
End Point Monitor 1526
User Quota Monitor 1527
Application Block 1527
Summary 1527
Application 1528

User/IP 1529
Statistical Period 1529
iQoS Monitor 1530
Device Monitor 1530
Summary 1531
Statistical Period 1534
Detailed Information 1535
Online IP 1537
Keyword Block 1538
Summary 1538
File Content 1539
Web Content 1539
Email Content 1540
Web Posting 1540
User/IP 1540
Statistical Period 1541
Locking User 1541
Locking IP 1542
Authentication User 1544
URL Hit 1544
Summary 1544
User/IP 1545

URL 1546
URL Category 1547
Statistical Period 1548
Link Status Monitor 1548
Link User Experience 1548
Statistical Period 1550
Link Detection 1550
Detection Destination 1553
Link Configuration 1555
IoT Monitor 1556
Summary 1556
Screening Monitoring Mode 1557
Details 1558
Monitor Configuration 1560
Long-term Monitor 1562
Long-term Monitor Configuration 1563
Long-term Monitor Statistics 1564
Long-term Monitor Storage Size Settings 1568
Logging 1568
Log Severity 1569
Destination of Exported Logs 1570
Log Format 1571

Event Log 1571
Network Log 1571
Configuration Log 1572
Share Access Logs 1572
Threat Log 1573
Session Log 1577
PBR Log 1579
NAT Log 1579
URL Log 1581
EPP Log 1581
IoT Log 1582
File Filter Log 1582
Content Filter Log 1583
Network Behavior Record Log 1584
CloudSandBox Log 1584
Endpoint Tag Log 1585
Managing Logs 1587
  Configuring Logs 1587
    Option Descriptions of Various Log Types 1587
Log Configuration 1602
  Configuring a Log Server 1602
    Creating a Log Server 1602

Configuring Sending Souceport Number 1605
Configuring Log Encoding 1606
Adding Email Address to Receive Logs 1607
Facility Configuration 1607
Specifying a Mobile Phone 1608
Reporting 1609
Report File 1609
Report Template 1610
Creating a User-defined Template 1611
Editing a User-defined Template 1615
Deleting a User-defined Template 1616
Cloning a Report Template 1616
Report Task 1616
Creating a Report Task 1617
Editing the Report Task 1622
Deleting the Report Task 1622
Enabling/Disabling the Report Task 1623
Report Status 1623
NetFlow 1624
Configuring NetFlow 1624
Configuring a NetFlow Rule 1625
NetFlow Global Configurations 1627

Chapter 14 Diagnostic Center 1628
Packet Loss Statistics 1628
Packet Loss Statistics 1629
Packet Loss Details 1630
Module Threshold 1630
Packet Loss Statistics Storage Size Settings 1632
Statistical Period 1632
Packet Path Detection 1633
Configuring Packet Path Detection 1633
Emulation Detection 1633
Online Detection 1636
Imported Detection 1639
Detected Sources 1642
Packet Capture Tool 1642
Configuring Packet Capture Tools 1643
Create a Packet Capture Rule 1646
Packet Capture Global Configuration 1648
Test Tools 1650
DNS Query 1650
Ping 1651
Traceroute 1651
Debugging 1652

Failure Feedback 1652
System Debug Information 1652
Chapter 15 High Availability 1653
Basic Concepts 1656
HA Cluster 1656
HA Group 1656
HA Node 1656
Virtual Forward Interface and MAC 1656
HA Selection 1657
HA Synchronization 1657
Configuring HA Active-Passive (A/P) Mode 1659
HA Interface Traffic Monitor 1668
HA Manual Synchronization 1668
HA Session Synchronization 1670
HA Primary/Secondary Switchover 1670
Viewing the HA Status of the Device 1670
Configuring HA Peer Active-Active (A/A) Mode 1672
HA Interface Traffic Monitor 1680
HA Manual Synchronization 1682
HA Session Synchronization 1683
HA Primary/Secondary Switchover 1684
Viewing the HA Status of the Device 1684

Chapter 16 System Management 1685
System Information 1685
Viewing System Information 1686
Password-free Login to CLI via WebUI 1689
Device Management 1690
Administrators 1691
VSYS Administrator 1693
Configuring an Administrator 1695
Creating an Administrator Account 1695
Changing the Password for Admin Users 1699
Configuring Login Options for the Default Administrator 1700
Enabling Telnet/HTTP Login Type for the Default Administrator 1700
Admin Roles 1701
Trusted Host 1703
Creating a Trusted Host 1703
Management Interface 1706
System Time 1709
Configuring the System Time Manually 1709
Configuring NTP 1710
NTP Key 1712
Creating a NTP Key 1712
Option 1713

Rebooting the System 1717
System Debug 1717
Application Layer Security Bypass 1717
Storage Management 1718
Password Reset Management 1723
Security Authentication Management 1724
Startup Wizard 1726
Skipping the Startup Wizard 1727
Starting the Startup Wizard 1727
Configuration File Management 1734
Managing Configuration File 1735
Viewing the Current Configuration 1736
Importing/Exporting the Configuration of All VSYS 1737
Docker Management 1738
Operations about Docker Management 1739
Creating a Docker and Allocating System Resources 1739
Editing/Deleting a Docker 1741
Managing Image Files 1742
Managing a Container 1743
Docker Global Configuration 1743
Warning Page Management 1745
Page Management 1745

Uploading the Picture 1745
Editing the Picture 1746
Deleting the Picture 1746
Page Management 1747
SNMP 1750
SNMP Agent 1751
SNMP Host 1752
Trap Host 1755
V3 User Group 1756
V3 User 1758
Downloading MIB Files 1760
SNMP Server 1760
Creating an SNMP Server 1760
NETCONF 1762
Configuring the NETCONF Agent 1764
Configuring NETCONF Candidate 1764
Configuring NETCONF Timeout 1764
Extended Services 1765
Connecting to Centralized Management 1765
Connecting to HSM 1765
HSM Deployment Scenarios 1766
Connecting to CloudPano 1767

CloudPano Deployment Scenarios 1767
Connecting to Centralized Management 1769
Connecting to Hillstone Cloud Service Platform 1770
Configurations about Connecting to Hillstone Cloud Service Platform 1771
Connecting to Hillstone Cloud Service Platform 1771
Configuring CloudView 1774
Configuring Cloud Sandbox 1776
Configuring CloudVista 1777
Enabling Hillstone Cloud Service with One Click 1779
Connecting to iSource 1782
iSource Typical Deployment 1782
Stand-alone Deployment 1782
Cluster Deployment 1783
Connecting to iSource 1784
Configuring the Data Types Sent to iSource 1785
Upgrading System 1786
Upgrading Firmware 1787
Upgrading Database Data 1788
Updating Signature Database 1791
Updating Trusted Root Certificate Database 1794
License 1796
Applying for a License 1809

Installing a License 1809
Feedback Template 1810
Mail Server 1812
Creating a Mail Server 1812
SMS Parameters 1814
SMS Modem 1814
Configuring SMS Parameters 1815
Testing SMS 1815
SMS Gateway 1815
Configuring SMS Gateway 1815
Testing SMS 1827
SMS Parameters 1828
VSYS (Virtual System) 1828
VSYS Objects 1829
Root VSYS and Non-root VSYS 1829
Creating Non-root VSYS 1830
Viewing VSYS Configuration 1832
Configuring VSYS Quota 1832
Viewing VSYS Quota 1839
Resources 1840
Entering the VSYS 1841
Logging in to the Device by Using the API Token 1843

Creating an API Token 1843
Secure Connect Client Management 1844
Customizing Secure Connect Download Page 1845
Customizing Client Download Source 1846
The Maximum Concurrent Sessions 1847

Welcome

Thanks for choosing Hillstone products!

This part introduces how you get user guides of Hillstone products.

Hillstone provides the following guides to help you understand our products. Visit https://-docs.hillstonenet.com to download guides.

- Hillstone SG-6000 Hardware Reference Guide
- Hillstone Transceiver Module Reference Guide
- StoneOS WebUI User Guide
- StoneOS CLI User Guide
- StoneOS Cookbook
- StoneOS Getting Started Guide
- StoneOS Log Messages Reference Guide
- StoneOS SNMP MIB Reference Guide
- StoneOS Upgrade Guide
- CloudEdge Deployment Guide

Customer service hotline:

- Regions outside China: 1-800-889-9860
- Hong Kong (China): +852-55128899 (9:00 to 17:00 on every Monday to Friday)

Website: https://www.hillstonenet.com

Conventions

Know the operate method of WebUI common controls, can complete the configuration of most functions.

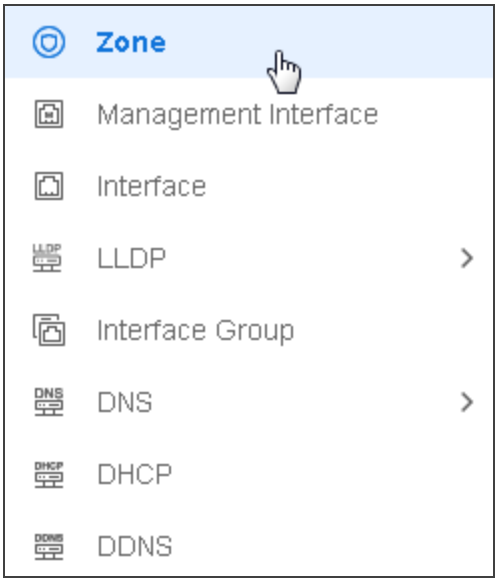
Note: All the configurations should be in UTF-8 code if not particularly indicated.

The common controls and effect of operating as follows:

- Switching between the function category : Select the tab (at the top of page).

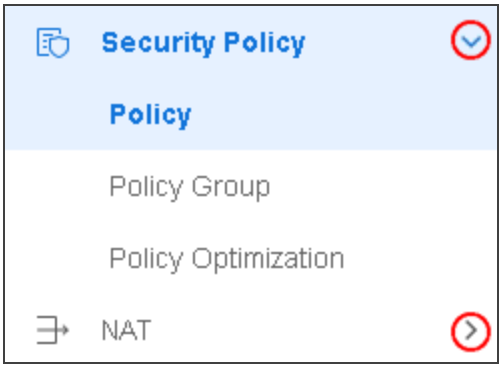


- Switching between the function : Click specific function node in level-2 navigation pane.

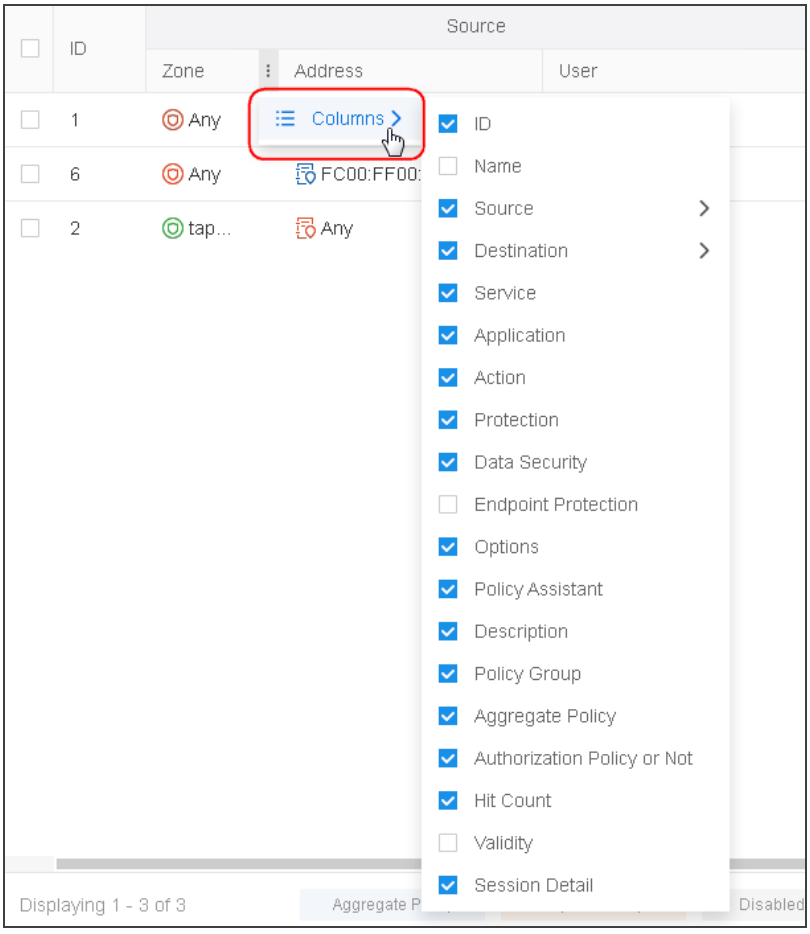


- Open the function list: Click ›in the level-2 navigation pane;

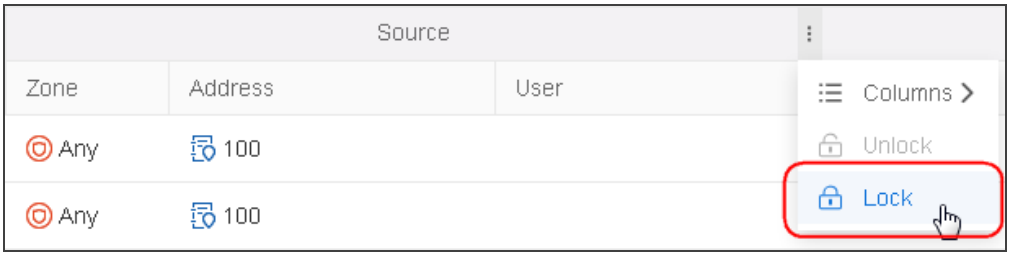
  Close the function list: Click ⌄ in the level-2 navigation pane.



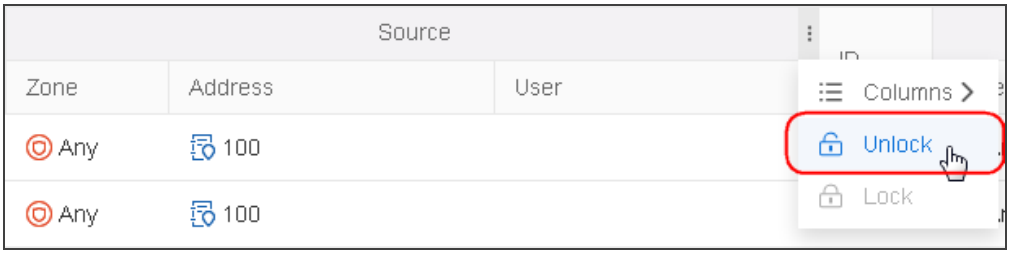
- Viewing the specified column: Click › icon, click "Column" in the drop-down list, select the specified list.The system support for the list status memory function, the system will display the last configuration of the list status when logging in to the device.



- To lock the column: Click ⋮ icon, click "Lock" in the drop-down list, the locked column will be always showing at the right of the list.



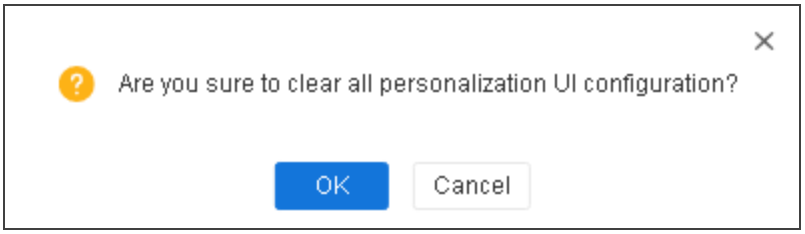
- To unlock the list: Click ⋮ icon, click "Unlock".



- To restore the initial state of the list: double-click the list header and click "OK" in the dialog box.

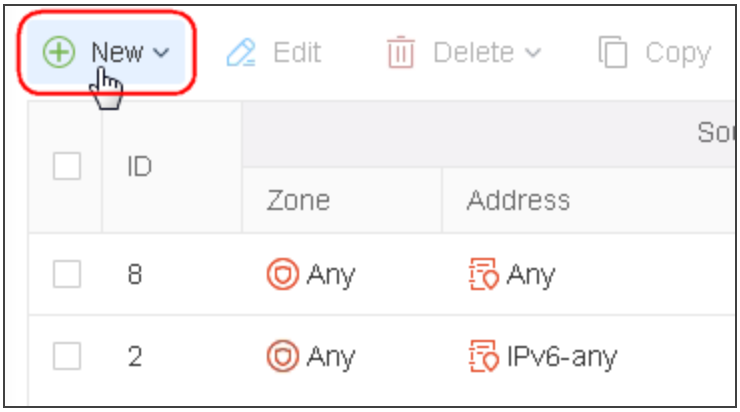


- To restore the initial state of all the list: Click › button of the user name in the top right corner of the page and click "OK" in the dialog box.

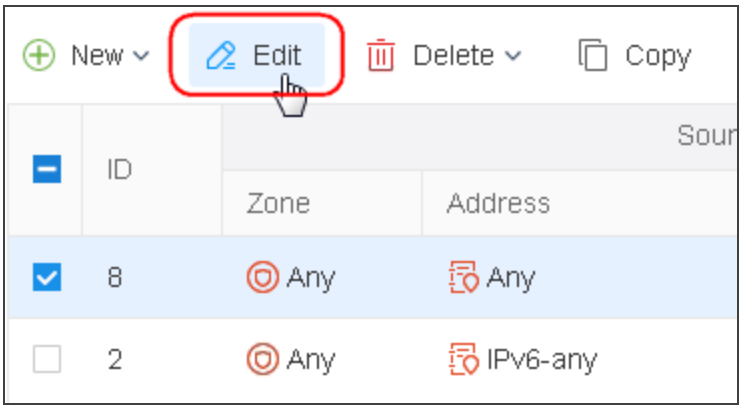


- To view the specified items by setting up filters: click Filter button, select filter conditions from the **Filter** drop-down list, and then select filter conditions as needed. To delete a filter condition, hover your mouse on that condition and then click the × icon. To delete all filter conditions, click the ×Remove All icon on the right side of the row.

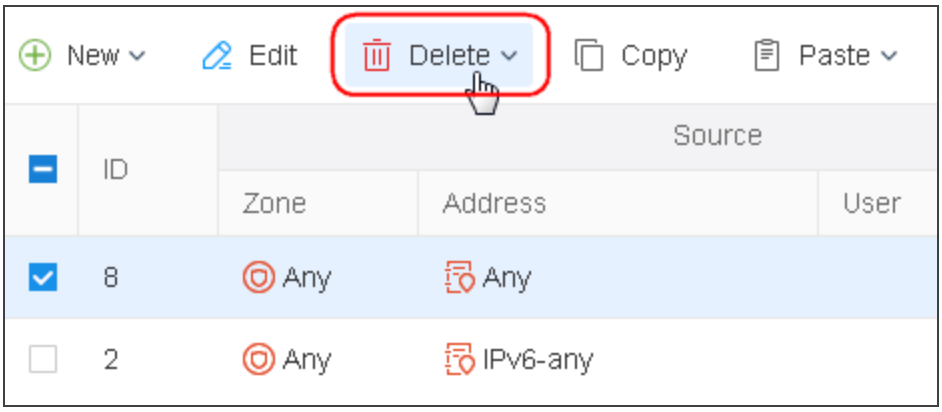
- To create a item, click **New**.



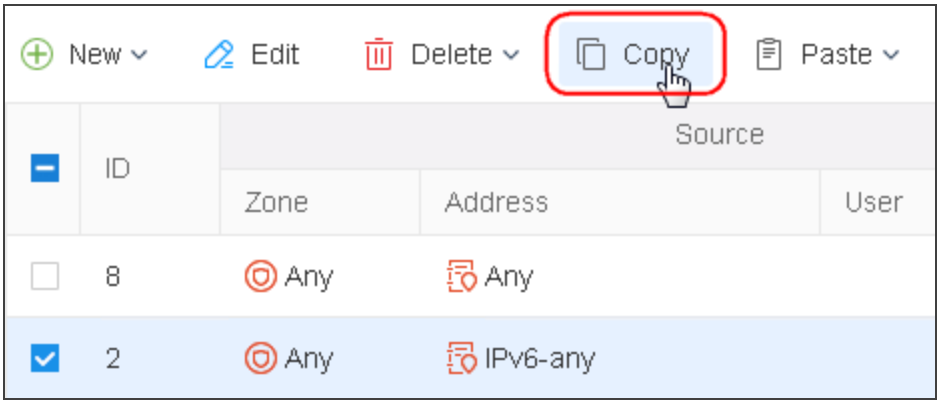
- To edit a item, select the check box and click **Edit**.



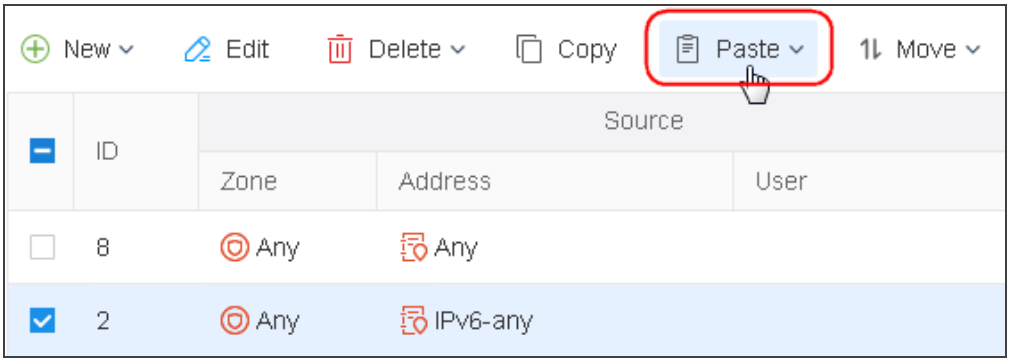
- To delete the items, select the check box and click **Delete**.



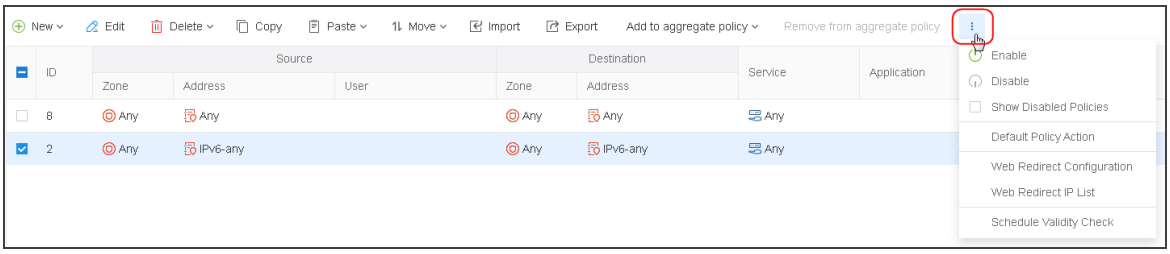
- To copy a item, select the check box and click **Copy**.



- To paste a item, select the check box and click **Paste**.



- To display the hidden controls , click ⋮.



- To update the data displayed on the current page, click **refresh**.



- To search according one condition , click **Filter**. In the pop-up line, click **+Filter** to add a new filter condition. Then select a filter condition from the drop-down menu and enter a value. And then press **Enter** to start searching.

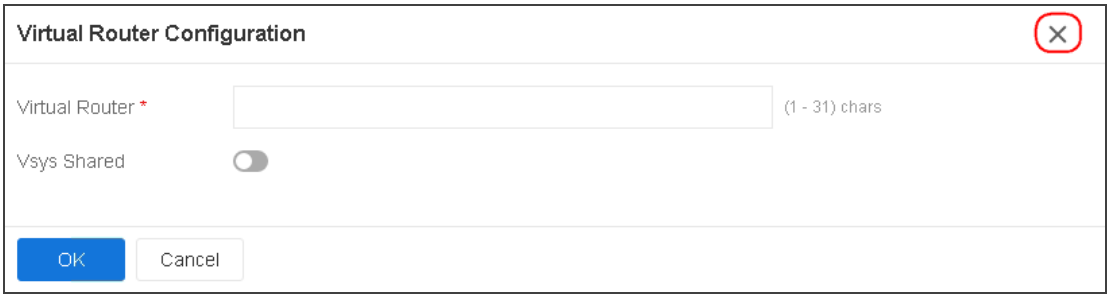


- To search according multiple conditions, click 

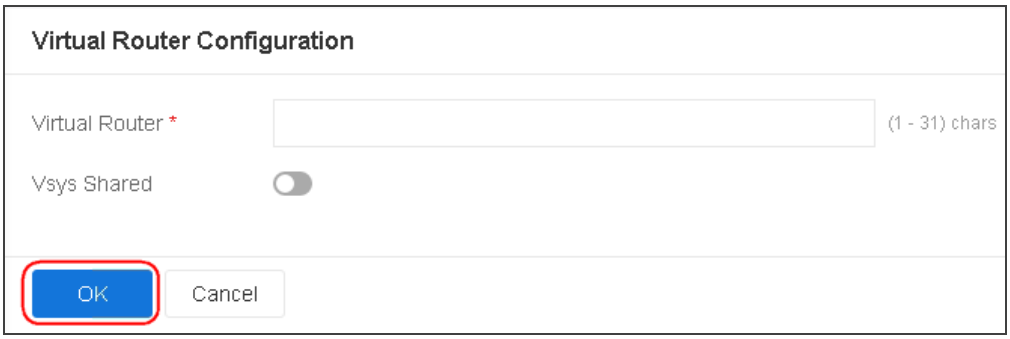
to add another filter condition, Then select a filter condition from the drop-down menu and enter a value. And then press **Enter** to start searching.



- To close the dialog, click 'X' at the top right corner of dialog.



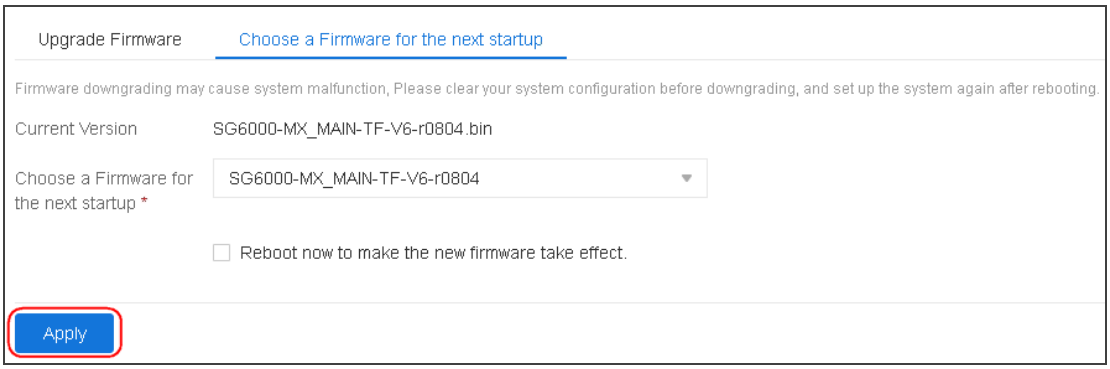
- To save the current configuration, click **OK**.



- To cancel the current operation, click **Cancel**.



- Click **Apply**, the modification will be took effect.



- Click next page buttons to jump to previous page , next page , dashboard or last page. Enter the page number, jump to the corresponding page.



Explorer Compatibility

The following browsers have passed compatibility tests:

- Microsoft Edge
- Chrome

Chapter 1 Getting Started Guide

This guide helps you go through the initial configuration and the basic set-up of your Hillstone device.

This guide is based on StoneOS 5.5R11. With system updates, the user interface is subject to change, and WebUI layout may vary depending on hardware platforms. This guide may not comply with every detail on your WebUI, please check your WebUI. The actual web pages take precedence.

1. "Log in to WebUI" on Page 12
2. "Startup Wizard" on Page 1726
3. "Preparing the StoneOS System" on Page 21, including:
    - Configuring the System Time
    - Installing Licenses
    - Creating a System Administrator
    - Adding Trust Hosts
    - Upgrading StoneOS Firmware
    - Configuring the DNS Server
    - Updating Signature Database
    - Connecting to the Internet
        - Connecting to the Internet Under Routing Mode
        - Connecting to the Internet Under Transparent Mode
        - Connecting to the Internet via mobile 3G/4G

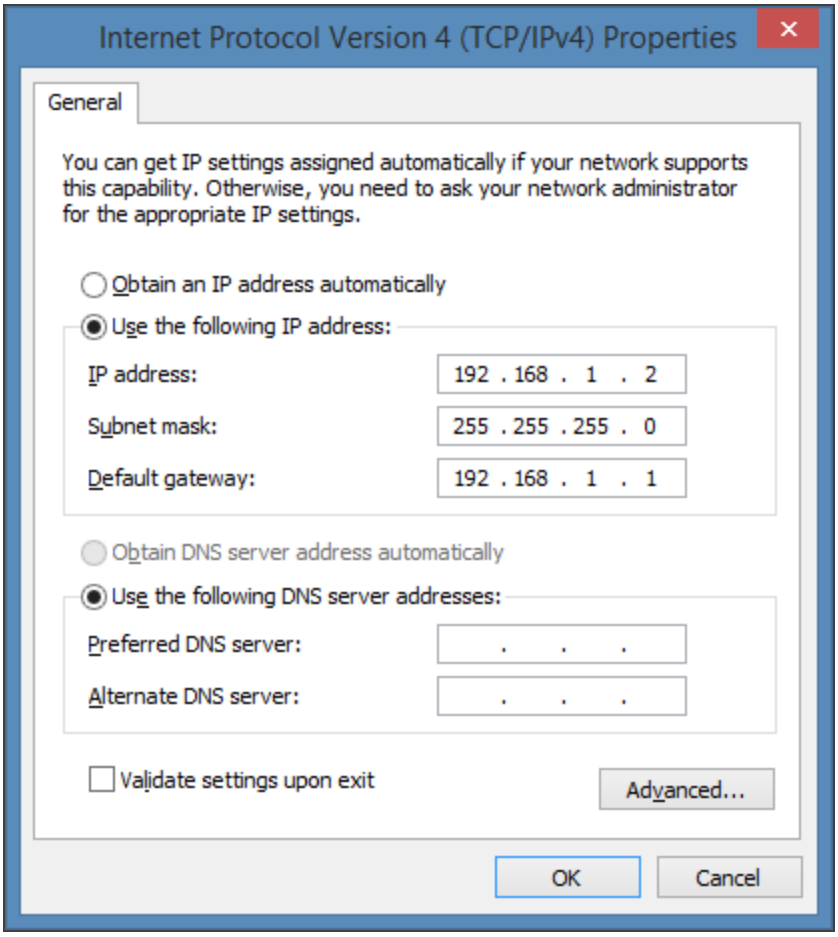
4. "Restoring Factory Settings" on Page 53
5. "General Features" on Page 55
    - Device Management
    - Threat Prevention
    - High Availability (HA)
    - Exporting Logs

Log in to WebUI

Interface ethernet0/0 is set with the default IP address 192.168.1.1/24. Meanwhile, the management services of SSH, PING, SNMP, and HTTP are all enabled for this interface (except for some custom versions). You can access the WebUI of the device through this interface at your initial visit to the device.

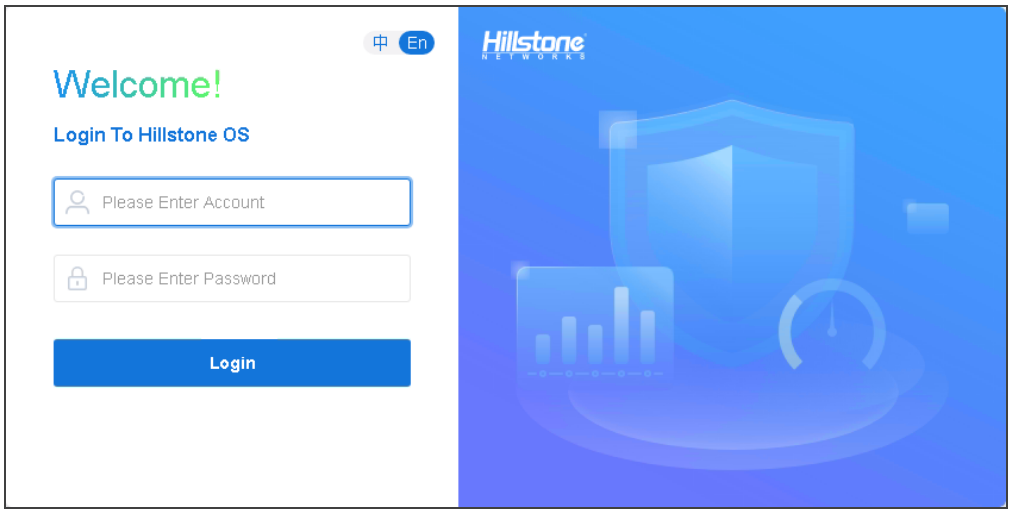
To visit the WebUI for the first time, take the following steps:

1. Go to your computer's Ethernet properties and set the IPv4 protocol as below.



2. Connect your computer to interface ethernet0/0 with an RJ-45 Ethernet cable.

3. In your browser's address bar, type "https://192.168.1.1" and press **Enter**.



4. On the login page, type the default username and password: hillstone/hillstone.

5. An EULA (end-user license agreements) is made available to you when you first log in to the WebUI. You need to read and accept EULA. Click **EULA** to view its details.

6. Click **Login**, follow the prompts to change the default password, and then log in again with the new password.

Startup Wizard

With the Startup Wizard, you can quickly complete the initialization configuration of the device without the need to delve into complex configuration details. This allows you to connect the device to the internet and achieve basic security protection.

After logging in to the firewall and changing the password via WebUI, you will be presented with a Startup Wizard. You can follow the steps to complete initial configuration of the firewall, including the host name, system time and license, routing mode deployment, and security policy configuration. You can also skip the Startup Wizard and configure the firewall.

Notes:

Under any of the following conditions, the Startup Wizard will not be prompted when the administrator logs in the WebUI:

- The firewall is deployed in HA mode;
- The login address does not point to the WebUI homepage, such as "http://x.x.x.x/#icenter";
- Logging in to the firewall WebUI on the HSM device;
- Logging in to the firewall WebUI via SSO on the cloud platform.

Skipping the Startup Wizard

To skip the Startup Wizard, take the following steps:

1. On the Startup Wizard welcome page, Click **Skip**.
2. The Skip page will be displayed, asking "Are you sure to skip the startup wizard?". You can select the **Do not display next-time login** check box as required. If this check box is not selected, the Startup Wizard will be displayed at your next login.
3. Click **OK** to close the Startup Wizard.

Starting the Startup Wizard

If the Startup Wizard is skipped, you can restart it again as follows:

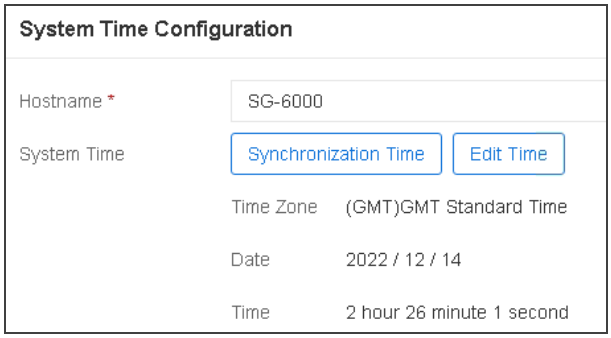
1. Select **System** > **Device Management** > **Startup Wizard**.
2. On the Startup Wizard page, configure whether to restore the device to factory defaults as required:

a. If **Restore to Factory Defaults** is enabled, the system will erase all system configuration after you start the Startup Wizard.

b. If **Restore to Factory Defaults** is disabled, the security policies created in the Startup Wizard have a higher priority than the policies (if any) previously configured in the Policy module. Other configuration, except policies, will be updated to the one configured in the Startup Wizard. By default, **Restore to Factory Defaults** is disabled.

3. Click **Open** to go to the Startup Wizard.

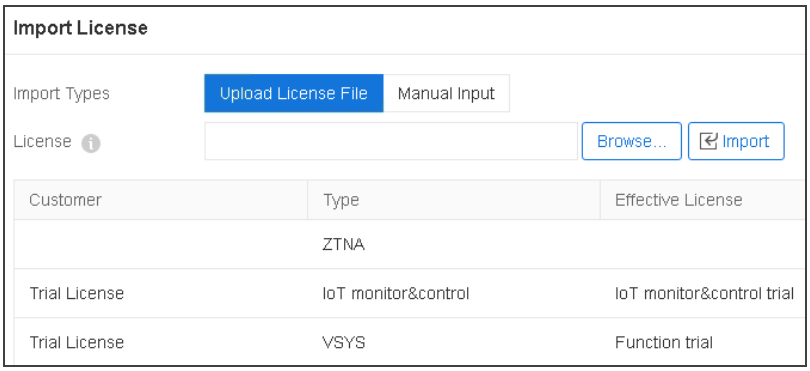
4. Click **Start Wizard** to start the Startup Wizard and enter the **System Time Configuration** page.



Option	Description
Hostname	Type the hostname. The value length is from 1 to 63 characters. The default value is SG-6000. Click **Next** to deploy the configuration.
System Time	Set the system time in either of the following ways: • Click **Synchronization Time** and the corresponding panel appears, where you can view your current timezone. Click **OK**. • Click **Edit Time,** and the corresponding panel appears,

Option	Description
	where you can set the timezone, date and time and then click **OK**.

5. Click **Next** to go to the **Import License** page.



Option	Description
Import Types	Specifies the method to import licenses. When licenses are imported, they are listed on the current page. Note that some licenses take effect only after a system restart. Please restart the system when Startup Wizard is fully configured. There are two ways of importing the licenses: • **Upload License File**: Click **Browse**, select the license that needs to be imported and then click **Import**. • **Manual Input**: Type the license content in the **License** text box and then click **Import**.

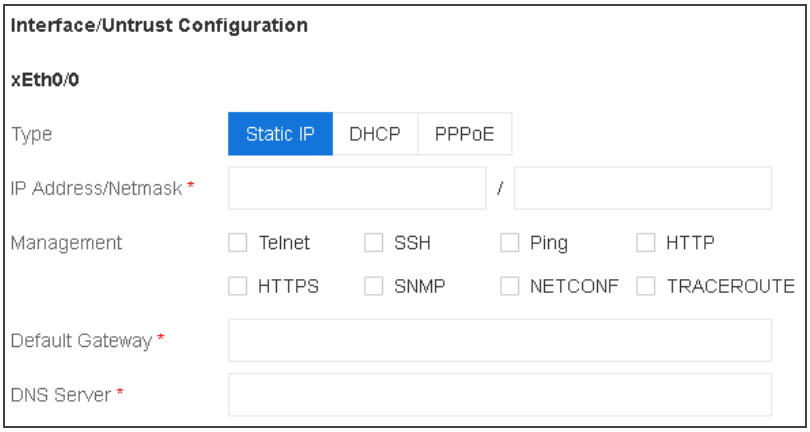
6. Click **Next** to go to the **Network Configuration** page. Network configuration will be deployed when the Startup Wizard is fully configured. In the Network Configuration section, in addition to the configuration that you can manually add in the Startup Wizard, the

system automatically configures an SNAT rule that enables the Sticky function, translating the Intranet IP to the IP address of the Intranet exit IP.



Option	Description
Untrust	Select the Internet interface and add it to the untrust zone.
Trust	Select the Intranet interface and add it to the trust zone.

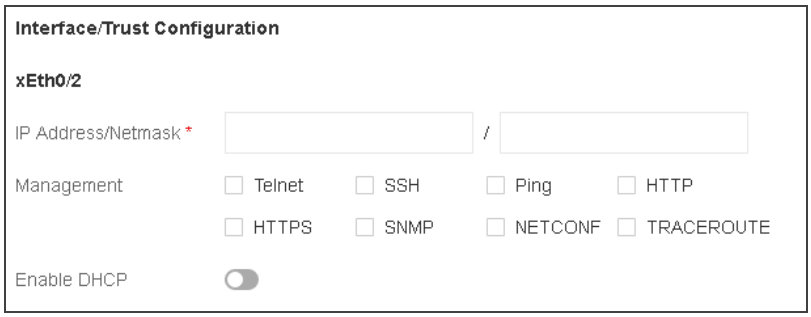
7. Click **Next** and configure the Internet interface.



Option	Description
Type	Select the method of obtaining IP addresses for the Internet interface.
Static IP	Specifies the IP address and netmask for the interface when **Static IP** is selected.
DHCP	When DHCP is selected, the interface will automatically obtain IP addresses using DHCP.
PPPoE	When PPPoE is selected, configure the following parameters:

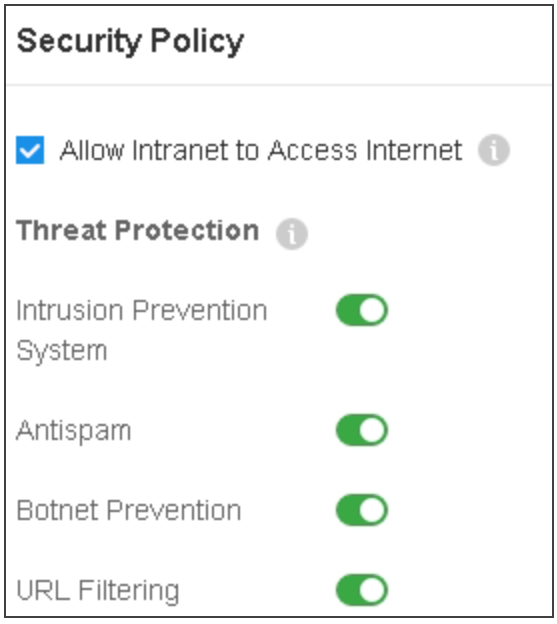
Option	Description
	• User: Specifies the PPPoE user name. The value length is from 1 to 31 characters. • Password: Specifies the password of the PPPoE user. The value length is from 1 to 31 characters. • Confirm Password: Type the password again. • Idle Interval: Specifies the idle interval. The uint is in minutes. The value range from is 0 to 10,000 minutes. When the idle time of the PPPoE interface reaches the specified value, the system will terminate the connection. By default, the value is 0, meaning the connection will not be terminated by the system. • Reconnect Interval: Specifies the interval after which the system will automatically reconnect after a disconnection The unit is in seconds. The value range is from 1 to 10,000 seconds.
Management	Specifies the interface management method, including Telnet, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.
Default Gate-way	Specifies the default gateway address.
DNS Server	Specifies the DNS server address.

8. Click **Next** to configure the Intranet interface.



Option	Description
IP Address/Net-mask	Specifies the IP address and netmask of the interface.
Management	Specifies the interface management method, including Tel-net, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.
Enable DHCP	After DHCP service is enabled, the interface will be con-figured as a DHCP server.
DHCP lease range	Specifies the address pool range. After the interface is con-figured as a DHCP server, the system will assign IP addresses from the address pool to the hosts, attempting to connect the interface.

9. Click **Next** to go to the **Security Policy** page. Security policy configuration will be deployed when the Startup Wizard is fully configured.



Option	Description
Allow Intranet to Access Internet	Select this check box to configure a security policy from the source zone (trust) to the destination zone (untrust), which will allow Intranet users to access the Internet. If this check box is not selected, the security policy will not be created.
Threat Protection	After **Allow Intranet to Access Internet** is selected, enable threat prevention functions as required. The threat prevention functions take effect only after corresponding licenses are imported. Initially, enabled threat prevention functions apply their default profile. To configure specific profiles, navigate to related modules after the Startup Wizard is fully configured. Note that some

Option	Description
	licenses take effect after a system reboot.

10. Click **Next** to go to the **Connecting to Hillstone Cloud Service Platform** page. Select the **Join the User Experience Program** check box to connect the system to the default Hillstone Cloud Platform account. This way, the system obtains broader threat intelligence so as to improve its protection capability.



11. Click **Next** to go to the **Options** page. You can view all configurations configured via the Startup Wizard.

12. Make sure the configurations are correct. Click **OK** to deploy network configuration and security policy configuration.

Preparing the StoneOS System

After logging in to the firewall through WebUI for the first time, you can configure the StoneOS system by customizing the following initial configuration.

- Configuring the System Time
- Installing Licenses
- Creating a System Administrator
- Adding Trust Hosts
- Upgrading StoneOS Firmware
- Configuring the DNS Server

- Updating Signature Database
- Connecting to the Internet

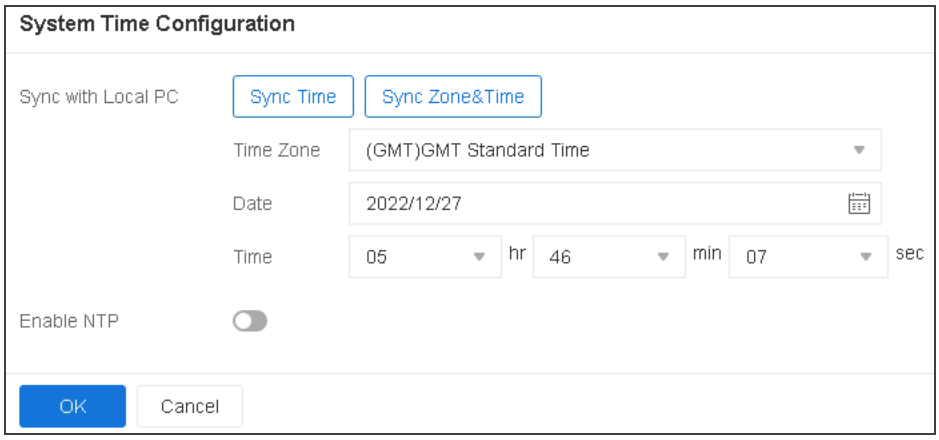
Configuring the System Time

System time affects many functional modules, such as the establishment of VPN tunnel, the functioning of schedule, and log time. Therefore, it is important to ensure the accuracy of the system time. You can configure the current system time manually, or synchronize the system time with the NTP server time via NTP protocol.

Configuring the System Time Manually

To configure the system time manually, take the following steps:

1. Select **System** > **Device Management** > **System Time**.
2. Configure the following options in the System Time Configuration section.



Option	Description
Sync with Local PC	Specifies the method of synchronizing with local PC. You can select **Sync Time** or **Sync Zone&Time**. • Sync Time: Synchronize the system time with local PC.

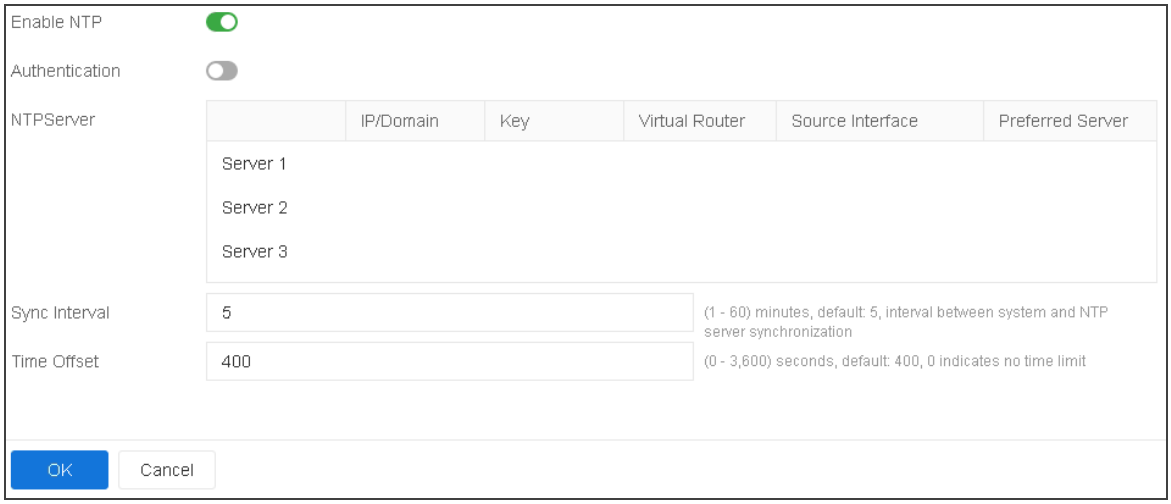
Option	Description
	• Sync Zone&Time: Synchronize the system zone&time with local PC.
-	Configure parameters of the system time. • Time Zone: Select the time zone from the drop-down list. • Date: Specifies the date. • Time: Specifies the time.

3. Click **OK**.

Configuring NTP

To configure NTP, take the following steps:

1. Select **System** > **Device Management** > **System Time**.
2. Configure the following options in the Enable NTP section.



Option	Description
Enable NTP	Click the button to enable the NTP function. By default, the

Option	Description
	NTP function is disabled.
Authentication	Click the button to enable the NTP Authentication function.
NTP Server	Specifies the NTP server that the device needs to synchronize with. You can specify at most 3 servers. • IP/Domain: Type IP address or domain of the server . • Key: Specifies the key that can be authenticated by this server. If you enable the NTP Authentication function, you must specify a key. • Virtual Router: Specifies the Virtual Router of interface for NTP communication. • Source Interface: Specifies an interface for sending and receiving NTP packets. • Preferred Server: Click the **Preferred Server** check box to set the server as the preferred server. The system will synchronize with the preferred server first.
Sync Interval	Type the interval value. The device will synchronize the system time with the NTP server at the interval you specified to ensure the system time is accurate.
Time Offset	Type the time value. If the time difference between the system time and the NTP server's time is within the max adjustment value you specified, the synchronization will succeed. Otherwise, it will fail.

3. Click **OK**.

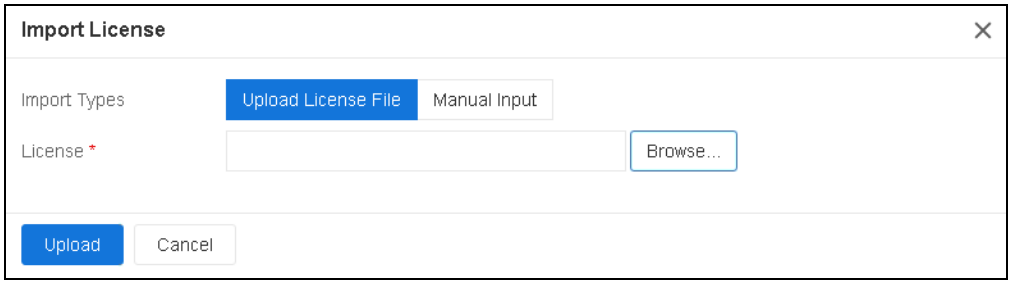
Installing Licenses

Licenses control features and performance.

Before installing any license, you must purchase a license code.

To install a license, take the following steps:

1. Go to **System > License**.
2. Click Import to open Import License page. Choose one of the three ways to import a license:



   - **Upload License File:** Select the radio button, click **Browse**, and select the license file (a .txt file).
   - **Manual Input**: Select the radio button, and paste the license code into the text box.

3. Click **OK**.
4. To make the license take effect, reboot the system. Go to **System > Device Management > Options**, and click **Reboot**.

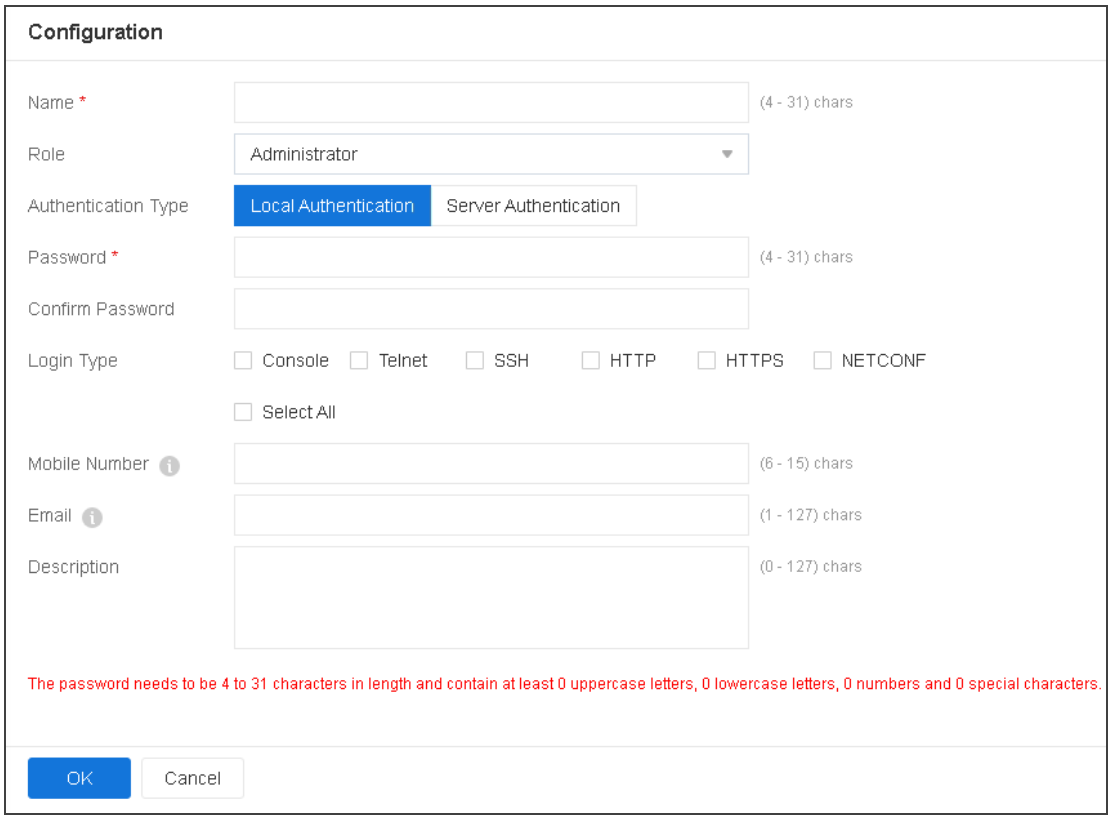
Creating a System Administrator

System administrator has the authority to read, write and execute all the features in the system.

To create a system administrator, take the following steps:

1. Go to **System > Device Management > Administrator**.

2. Click **New**.



Option	Description
Name	Type a name for the system administrator account.
Role	From the **Role** drop-down list, select a role for the administrator account. Different roles have different privileges. • Administrator: Permission for reading, executing and writing. This role has the authority over all features. • Operator: This role has the authority over all features except modifying the Administrator's configurations, and has no permission to check the log information

Option	Description
	• Auditor: You can only operate on the log information, including the view, export and clear. • Administrator-read-only: Permission for reading and executing. You can view the current or historical configuration information.
Authentication Type	Select the authentication type, including: • Local Authentication: When an administrator accesses StoneOS, the administrator is authenticated based on the administrator information (including the account and password) configured in StoneOS. • Server Authentication: When an administrator accesses StoneOS, the administrator is authenticated based on the administrator information (including the account and password) configured on the authentication server.
Authentication Server	If **Authentication Type** is set to **Server Authentication**, you need to select an authentication server from the drop-down list or click ⊕ button to create an authentication server. For details, see AAA Server. The following servers are supported: • Radius Server • Active Directory Server • LDAP Server • TACACS+ Server

Option	Description
Retry Local	After this function is enabled, local password verification will be performed if the server is unreachable. If the server returns a password error, this function is invalid. By default, the function is disabled.
Password	Type a login password for the admin into the **Password** box. The password should meet the requirements of Password Strategy.
Confirm Password	Re-type the password into the **Confirm Password** box.
Login Type	Select the access method(s) for the admin, including Console, Telnet, SSH, HTTP, HTTPS and NETCONF. If you need all access methods, select **Select All**.
Description	Enter descriptions for the administrator account.

3. Click **OK**.

Notes: The system has a default administrator "hillstone". You can modify the setting of hillstone.

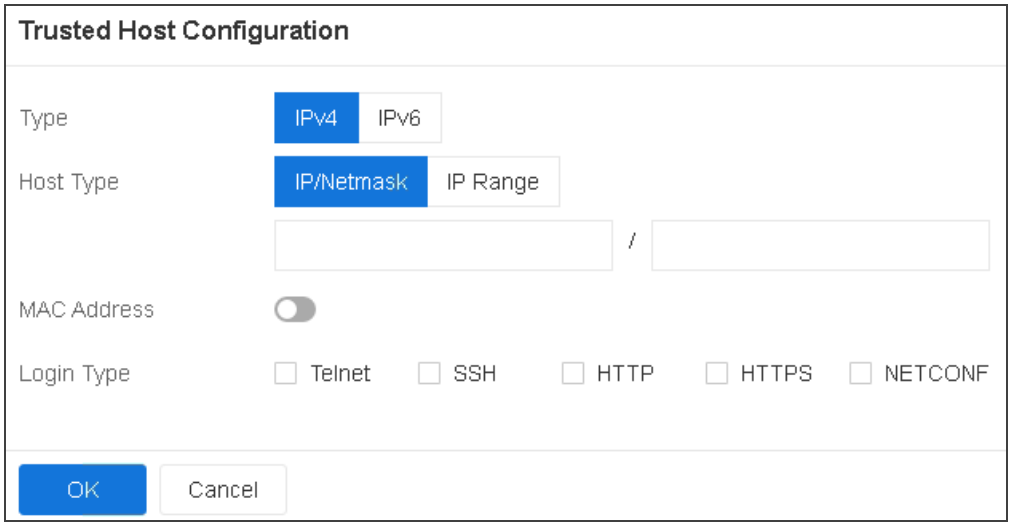
Adding Trusted Hosts

The trusted host is used to further ensure system security. An administrator can specify a trusted host by specifying the IP range or MAC address/MAC range. That's to say, hosts within the specified range are trusted hosts. Only computers included in the trust hosts can manage the system.

Notes: After adding the trust host, delete the default trust host range "0.0.0.0/0". "0.0.0.0/0" indicates that all hosts are trust hosts.

To add a trust host, take the following steps:

1. Select **System** > **Device Management** > **Trusted Host**.
2. Click **New**.
3. In the Trusted Host Configuration dialog box, configure these values.



Option	Description
When the system is IPv4 version, configure the following options:	
Match Address Type	Select the address type to match the trusted host. • When "IPv4" is selected, you need to specify the IP range, and only the hosts in the IP range can be the trust hosts; • When "IPv4&MAC" is selected, you need to specify the IP range or MAC address/range, and only the hosts in the specified IP range and MAC range can be the trusted hosts.
IP Type	Specifies the IP range of the trusted hosts:

Option	Description
	• IP/Netmask: Type the IP address and netmask of the trusted hosts. • IP Range: Type the start IP and end IP of the trusted hosts.
MAC Type	Specifies the MAC address or MAC range of the trusted hosts: • MAC Address: Type the MAC address of the trusted hosts. • MAC Range: Type the start MAC address and end MAC address of the trusted hosts.
Login Type	Select the access methods for the trusted host, including "Telnet", "SSH", "HTTP", "HTTPS", and "NETCONF".
When the system is IPv6 version, configure the following options:	
Type	Select the address type to match the trusted host: "IPv4" or "IPv6".

Host Type	Configure the IPv6 trusted host or the IPv4 trusted host.
	• If the user chooses "IPv4" type, specifies the IP address or the IP range of the IPv4 trusted host:
	  • IP/Netmask: Type the IP address and netmask of the trusted hosts.
	  • IP Range: Type the start IP and end IP of the trusted hosts.

Option	Description

	• If the user chooses "IPv6" type, specifies the IPv6 address or the IPv6 range of the IPv6 trusted host:
	  • IPv6/Prefix: Type the IPv6 address and prefix of the trusted hosts.
	  • IPv6 Range: Type the start IPv6 address and end IPv6 addressof the trusted hosts.

MAC Type	Click the **Enable** button to use the MAC address or the MAC range to match the trusted host. By default, this button is disabled.
MAC Address	Specifies the MAC address or the MAC range of the trusted host. • MAC address: Type the MAC address of the trusted hosts. • MAC range: Type the start MAC address and end MAC address of the trusted hosts.
Login Type	Select the access methods for the trust host, including "Telnet", "SSH", "HTTP", "HTTPS", and "NETCONF".

4. Click **OK**.

Upgrading StoneOS Firmware



Notes: Back up your configuration files before upgrading your system.

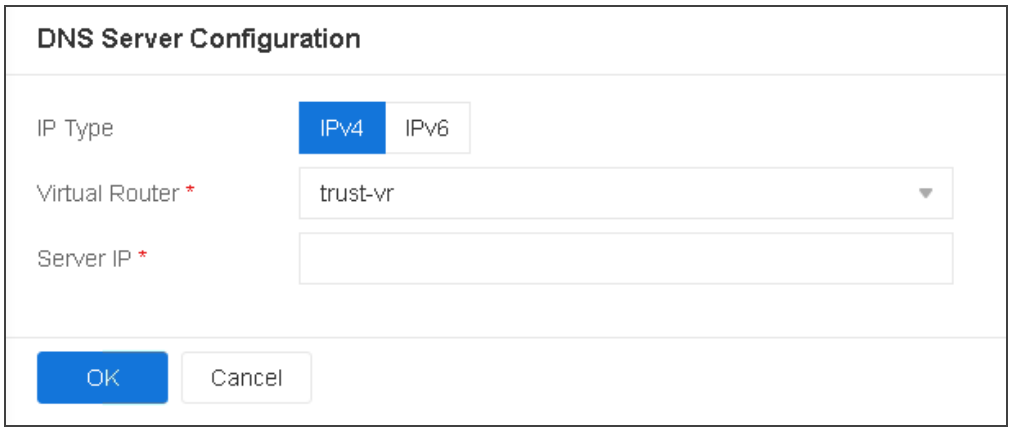
To upgrade your system firmware, take the following steps:

1. Go to **System > Upgrade Management**.
2. Select **Browse** and choose the new image from your local computer.
3. Click **Reboot to make new firmware take effect**, then click **Apply**.
4. System will automatically reboot when it finishes installing the new firmware.

Configuring a DNS Server

You can configure a DNS server for system to implement DNS resolution. To create a DNS server, take the following steps:

1. Select **Network > DNS > DNS Server**.
2. Click **New** in the DNS Server section.



3. Select the IP address type, including IPv4 or IPv6.
4. Select a VRouter from the VR drop-down list. The default VRouter is trust-vr.
5. Type the IP address for the DNS server into the Server IP box.
6. Click **OK**.

Updating Signature Database

By default, the system will automatically update the databases every day.

Notes:

- Features that require constant updates of signature are license controlled. You must purchase the license in order to be able to update the signature libraries.
- To ensure that the device connects to the default update server, configure the DNS server before the update.

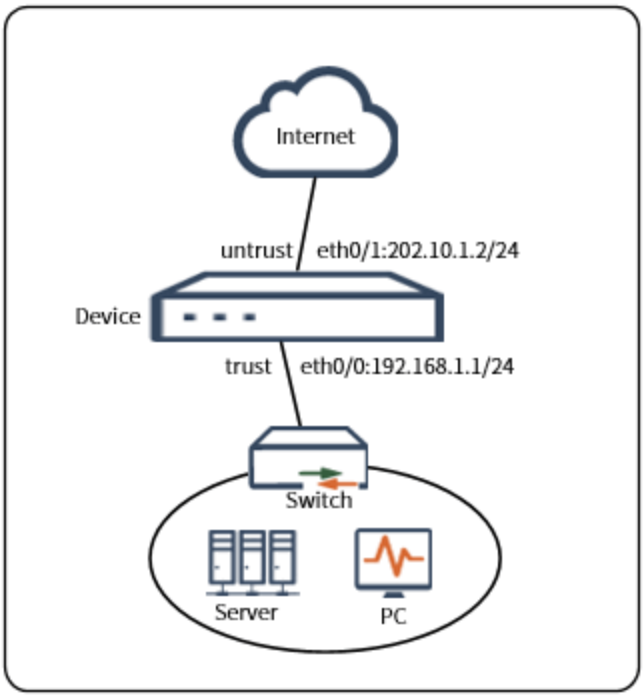
To update a database, take the following steps:

1. Select **System > Upgrade Management > Signature Database Update**.
2. Find your intended database, and choose one of the following two ways to upgrade.
   - **Remote Update**: Click **OK And Online Update** to immediately update the signature database. Or, enable **Auto Update** and specify the auto update time. The system will automatically update the signature database according to the configured update time. It is recommended to set the auto update time to the period of low service traffic.
   - **Local Update**: Select **Browse** to open the file explorer, and select your local signature file to import it into the system.

Connecting to the Internet

Connecting to the Internet Under Routing Mode

The routing mode often works with NAT. Therefore, the routing mode is also known as the NAT mode. In the routing mode, the device works as a gateway and router between two networks. This section shows how to connect and configure a new Hillstone device in the routing mode to securely connect the Intranet to the Internet.



To get your Intranet access to the Internet through a Hillstone device, take the following steps:

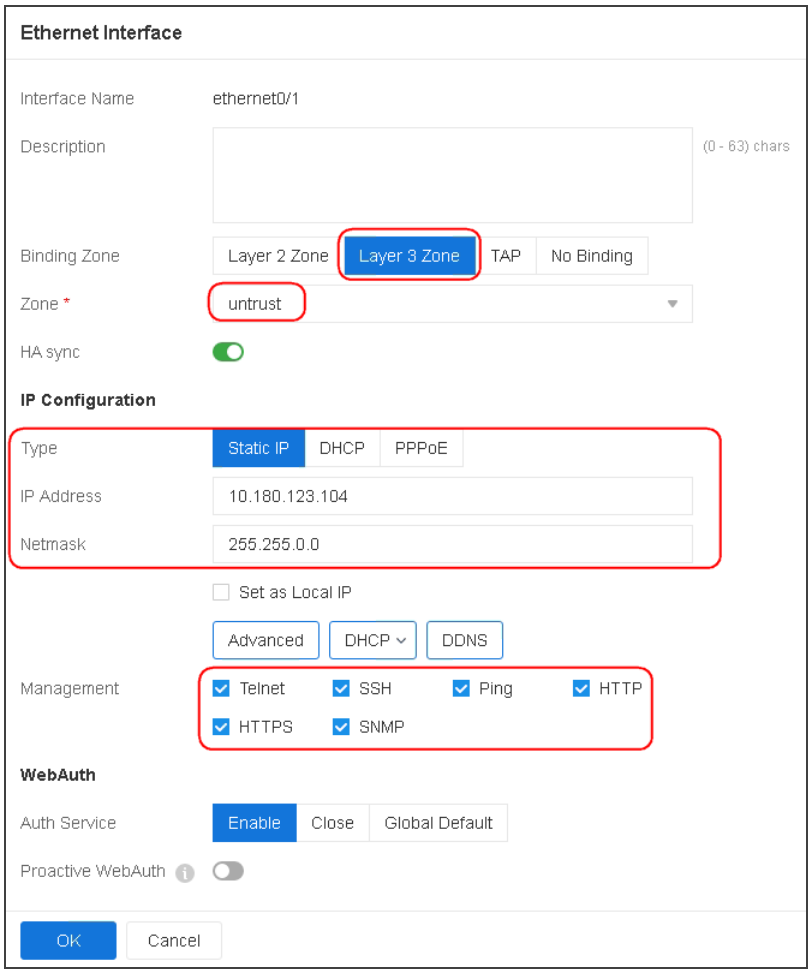
Step 1: Connecting to the device

1. Connect one port (e.g. ethernet0/1) of Hillstone device to your ISP network. In this way, "ethernet0/1" is in the untrust zone. Connect the Intranet to another Ethernet interfaces (e.g. ethernet0/0) of the device. This means "ethernet0/0" is connected to the trust zone.
2. Power on the Hillstone device and your PCs.
3. Access the system WebUI through the Intranet interface. For more information, refer to Log in to Web Interface.

Step 2: Configuring interfaces

1. Go to **Network > Interface**.

2. Double click **ethernet0/1**.



Option	Value
Binding Zone	L3-zone
Zone	untrust
IP Configuration	
Type	Static IP
IP Address	202.10.1.2 (public IP address provided by your ISP)
Netmask	255.255.255.0

Option	Value
Management	Select protocols that you want to use to access the device.
Interface Properties	
MTU	1500
ARP timeout	1200



Notes: Besides **Static IP**, you can also select the following types as needed in the **IP Configuration** section.

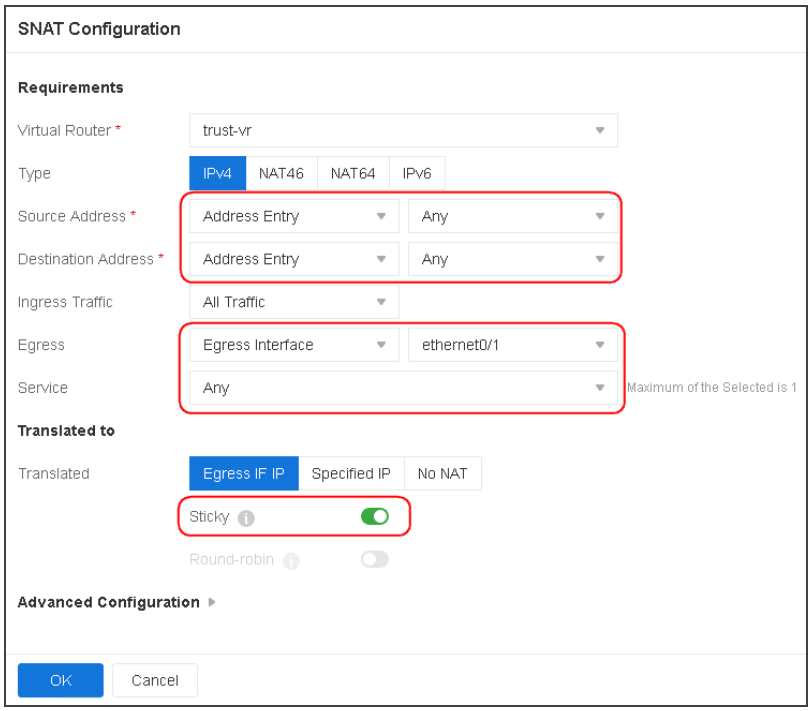
- DHCP: With DHCP selected, the interface automatically obtains an IP address through DHCP.
- PPPoE: With PPPoE selected, the interface obtains an IP address through PPPoE. In this case, you also need to configure the user name, password and confirm the password.

3. Click **OK**.
4. By default, ethernet0/0 belongs to the "trust" zone and is configured with 192.168.1.1/24. Therefore, there is no need to make further configuration.

Step 3: Creating a NAT rule to translate Intranet IP to public IP

1. Go to **Policy > NAT > SNAT**.

2. Click **New**



Option	Value
Requirements	
Virtual Router	trust-vr
Source Address	Address Entry, Any
Destination Address	Address Entry, Any
Egress	Egress interface, ethernet 0/1
Translated to	
Translated	Egress IP
Advanced Configuration	

Option	Value
ID	Automatically assign

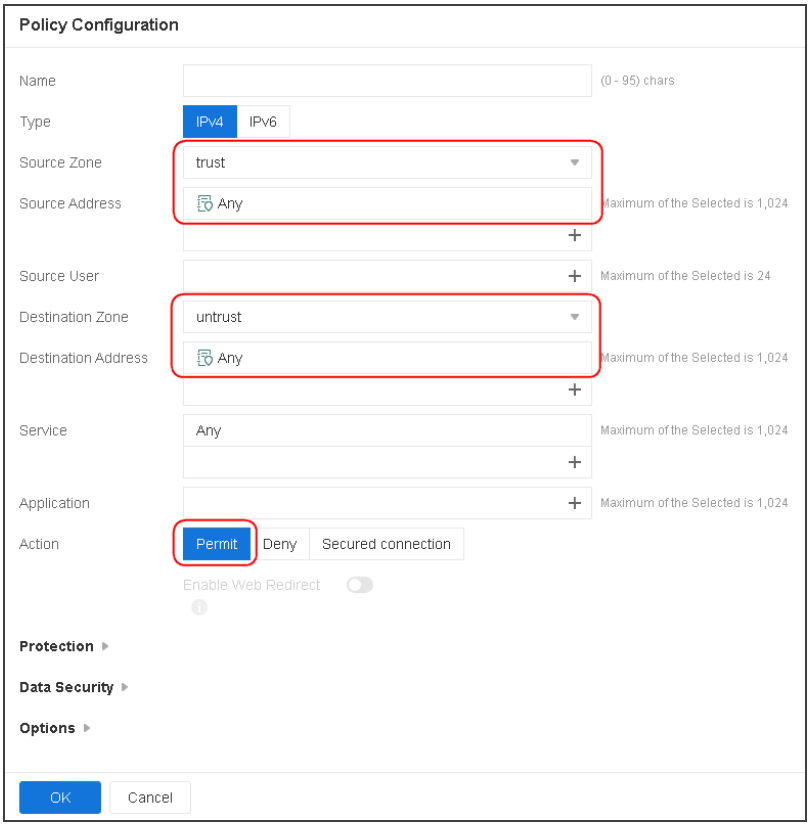
Notes: The egress interface should be specified as the Internet interface.

3. Click **OK**.

Step 4: Creating a security policy to allow internal users to access the Internet.

1. Go to **Policy > Security Policy> Policy**.

2. Click **New** and select **Policy** from the drop-down list.



Option	Value
Source Zone	trust

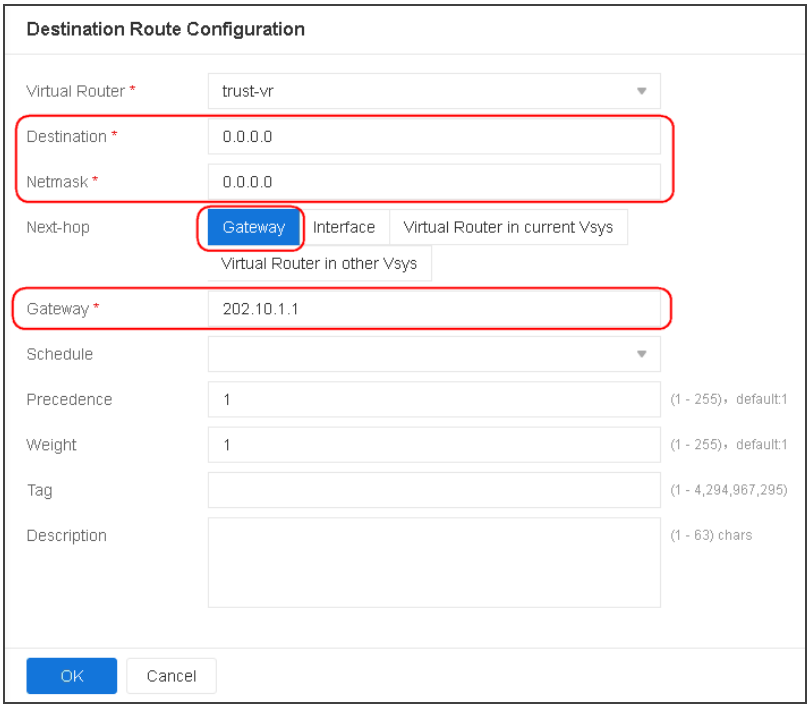
Source Address	Any
Destination Zone	untrust
Destination Address	Any
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

3. Click **OK**.

Step 5: Configuring a default route

1. Go to **Network >Routing > Destination Route**.

2. Click **New**.



Option	Value
Virtual Router	trust-vr

Option	Value
Destination	0.0.0.0 (means all network)
NetMask	0.0.0.0 (means all subnets)
Gateway	202.10.1.1 (gateway provided by your ISP)

3. Click **OK**.

Connecting to the Internet Under Transparent Mode

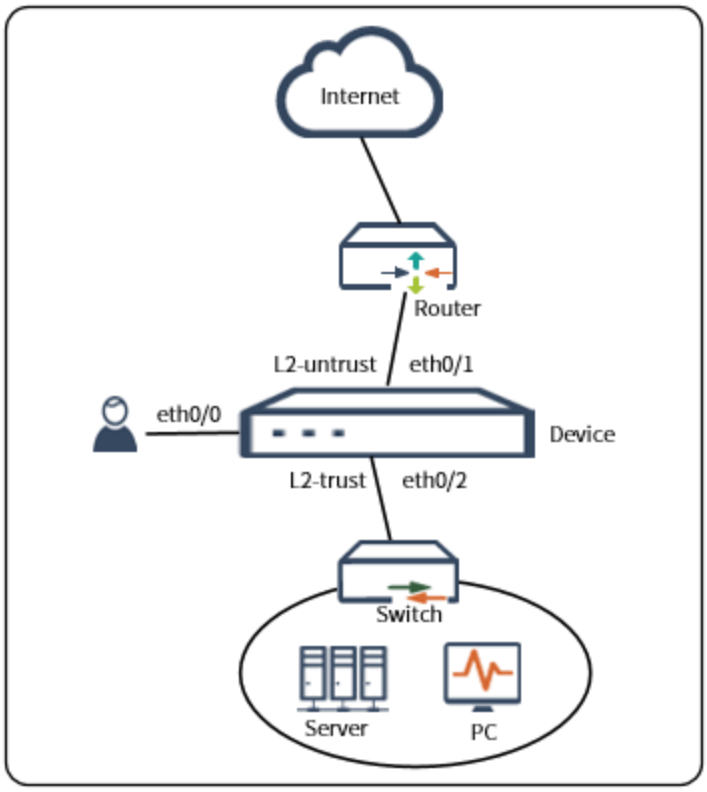
Transparent mode is also known as the bridge mode or transparent bridging mode. Transparent mode is used when the IT administrator does not wish to change the existing network layout. Normally, the existing network has already set up routers and switches. The firewall will be used as a security device.

Transparent mode has the following advantages:

- No need to change IP addresses
- No need to set up NAT rule

Under normal circumstances, the firewall in transparent mode is deployed between the router and the switch of the protected network, or it is installed between the Internet and a company's router. The Intranet uses its old router to access the Internet, and the firewall only provides security control features.

This section introduces a configuration example of a firewall deployed between a router and a switch. In this example, the administrator uses ethernet0/0 to manage firewall. The firewall's ethernet0/1 is connected to router (which is connecting to the Internet) and ethernet0/2 is connected to a switch (which is connecting to the Intranet).



Step 1: Connecting to the device

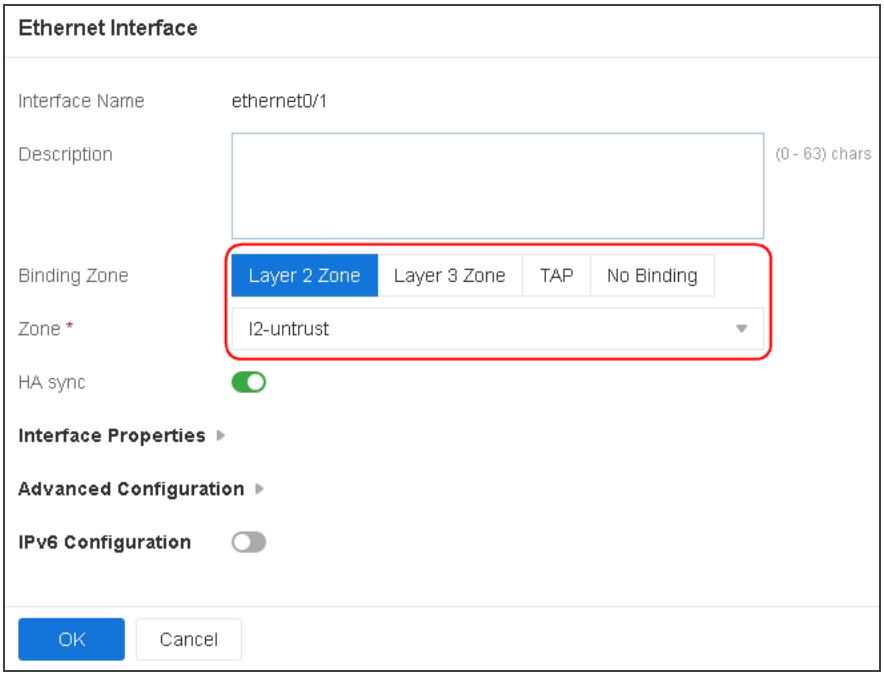
1. Connect one port (e.g. ethernet0/1) of Hillstone device to your ISP network. In this way, "ethernet0/1" is in the l2-untrust zone. Connect your Intranet to another Ethernet interfaces (e.g. ethernet0/2) of the device. This means "ethernet0/2" is connected to the l2-trust zone.
2. Power on the Hillstone device and your PCs.
3. Access the system WebUI through the Intranet interface. For more information, refer to Log in to Web Interface.

Step 2: Configuring interfaces

- Configure ethernet0/1 as an Internet connected interface.

    1. Go to **Network > Interface**.

    2. Double click **ethernet0/1**.



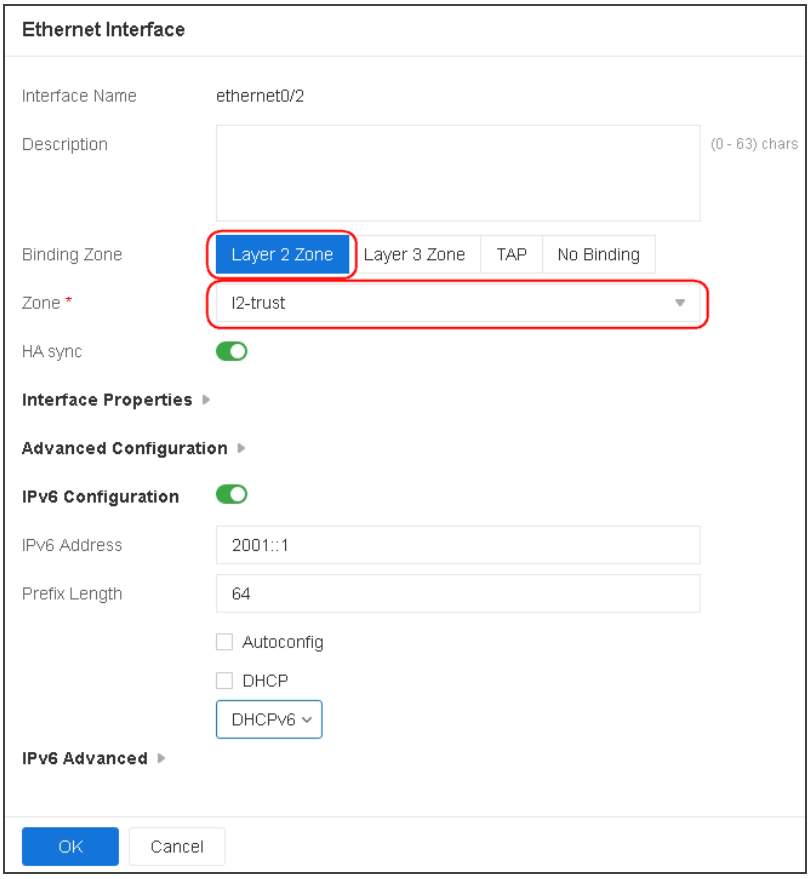
Option	Value
Binding Zone	L2-zone
Zone	l2-untrust

    3. Click **OK**.

- Configure ethernet0/2 as an Intranet connected interface.

    1. Select **Network > Interface**.

    2. Double click **etherneternet0/2**.



Option	Value
Binding Zone	L2-zone
Zone	l2-trust

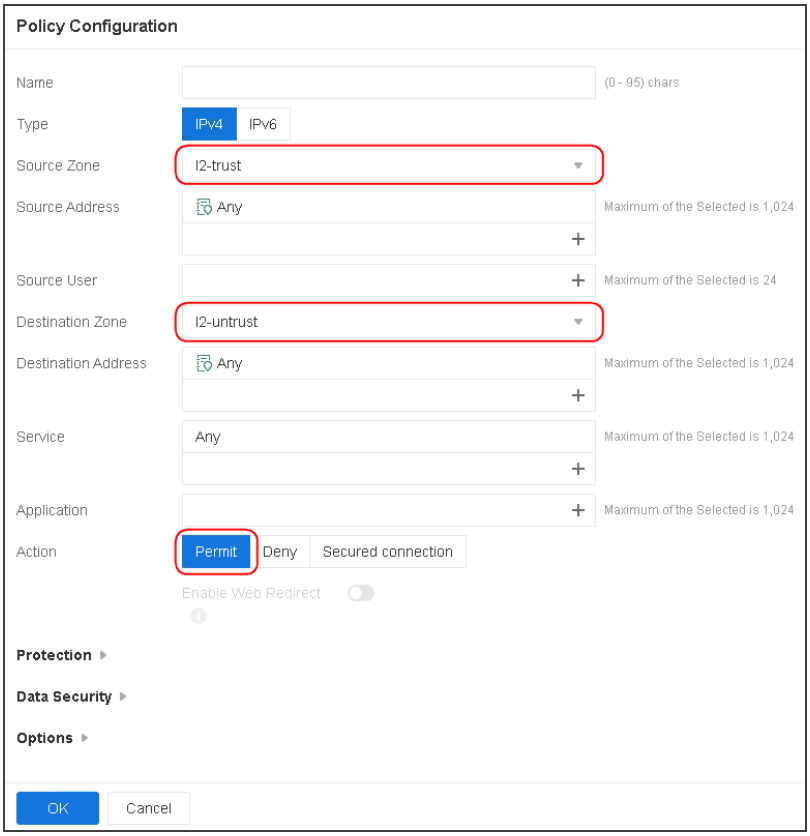
    3. Click **OK**.

Step 3: Configuring policies

- Create a policy to allow internal users to visit the Internet.

    1. Select **Policy > Security Policy>Policy**.

    2. Click **New**,select Policy from the drop-down list.



Option	Value
Source Zone	l2-trust
Source Address	Any
Destination Zone	l2-untrust
Destination Address	Any
Service/Service Group	Any

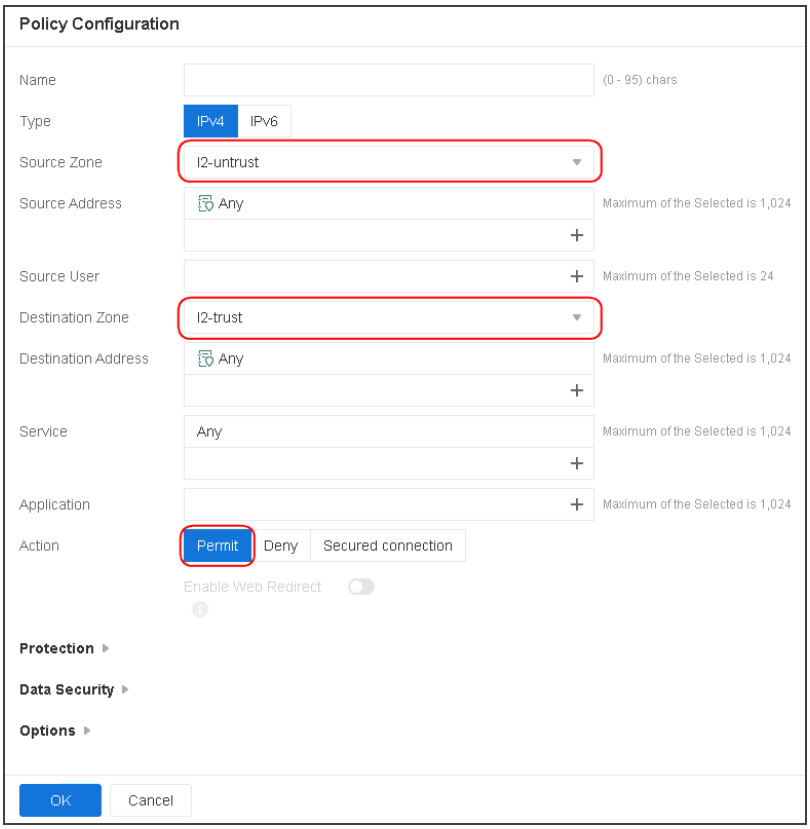
APP/APP Group	-----
Action	Permit

3. Click **OK**.

- Create a policy to allow the Internet to visit the Intranet.

1. Select **Policy > Security Policy**.

2. Click **New**.



Option	Value
Source Zone	ll2-untrust
Source Address	Any
Destination Zone	l2-trust

Destination Address	Any
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

3. Click **OK**.

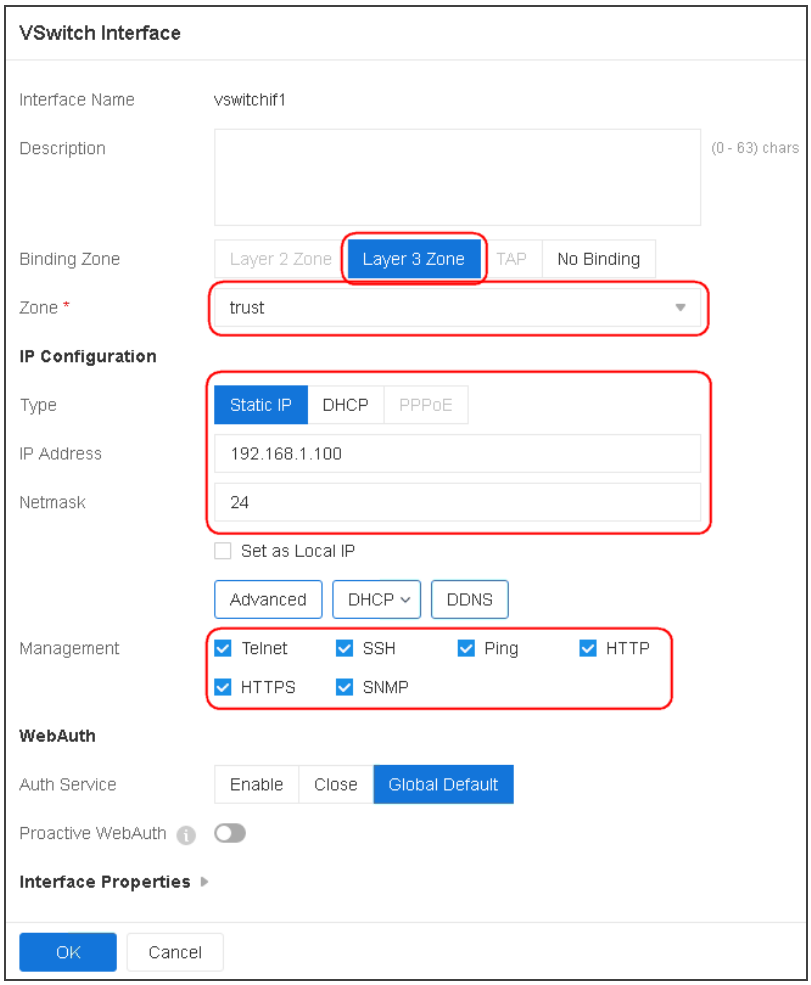
- The two policies above ensure communication between an Intranet and the Internet. If you want to set up more details, e.g. to limit P2P download, you can add more policies and place the new policies before the old ones. The match sequence of policies is determined by their position in the policy list, not their ID numbers.

(Optional) Step 4: Configuring VSwitch Interface for managing the firewall

If you want any PC in the Intranet to visit and configure the firewall, you can configure a VSwitch interface as a management interface.

1. Select **Network > Interface**.

2. Double click **vswtichif1**.



Option	Value
Binding Zone	Layer 3 Zone
Zone	trust
IP Address	192.168.1.100
Netmask	24
Management	Select SSH, Ping, and HTTPS

> **Notes:** When configuring **IP Configuration**, set an IP address in the same subnet of the Intranet.

3. Click **OK**.

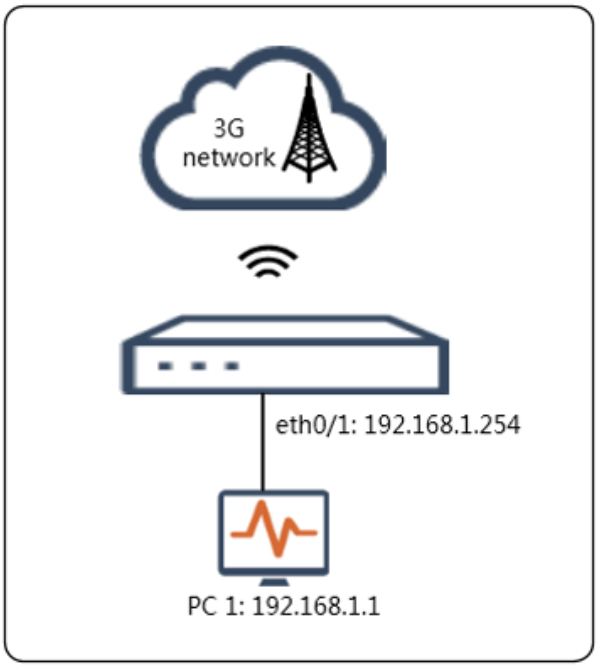
4. With any PC in the Intranet, enter the IP address of vswitchif1, and you will visit the firewall login WebUI.

Connecting to the Internet via mobile 3G/4G

When a device is equipped with 3G/4G data card and works in the routing mode, it can access the network through 3G/4G dial-up. Connecting to the Internet via 3G dial-up is similar to the one via 4G dial-up. Therefore, this sections takes 3G dial-up as an example.

> **Notes:** Obtain the following 3G parameters from IPS: access point, username, password, dial-up string.

The example introduced in this section is based on the following topology.



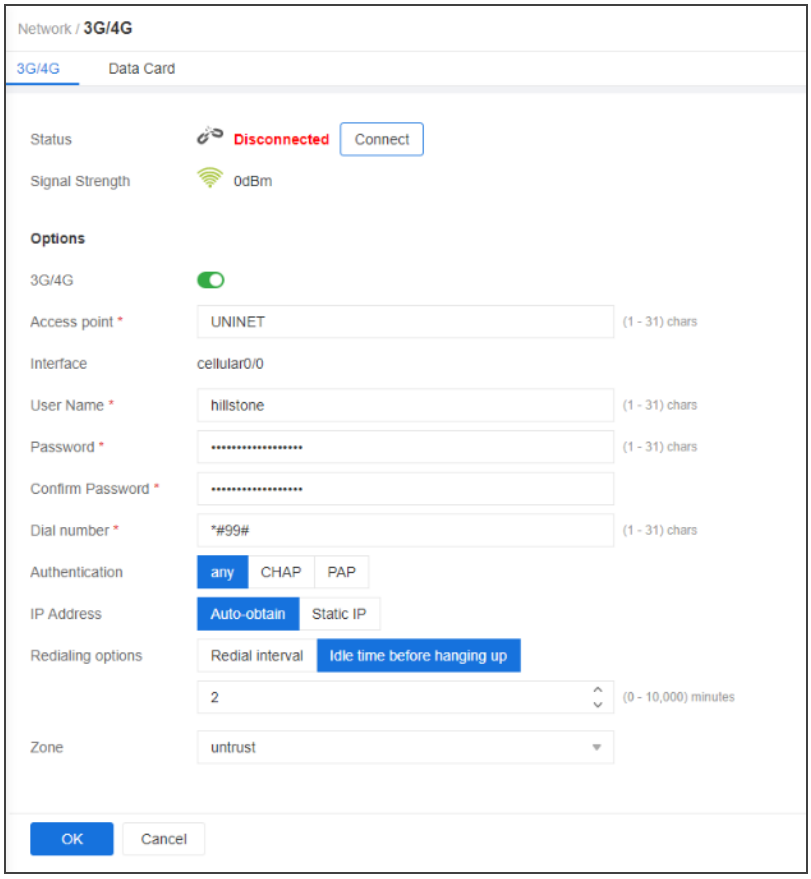
Step 1: Inserting the 3G Data card

Insert the 3G data card into the SIM card slot of the device.



Setp 2: Configuring 3G Parameters

1. Select **Network** > **3G/4G**



On the 3G/4G tab, enter values.

Option	Value
3G/4G	Click the button to enable the 3G
Access point	UNINET (WCDMA)

Option	Value
User name	hillstone
Password	123321
Confirm Pass-word	123321
Dial number	*99#
Authentication	any
IP Address	Auto-obtain
Redialing options	Idle time before hanging up
Zone	untrust

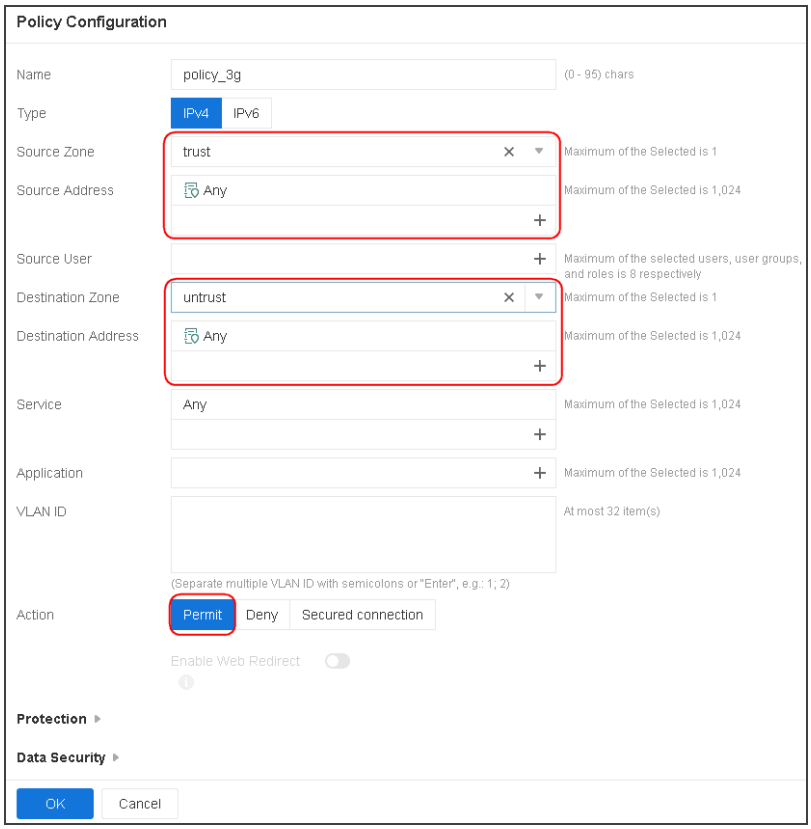
Step 3: Connecting 3G Network

On the 3G/4G tab, you can view the 3G/4G connection status in the Status section. Click **Connect** to connect to the 3G network.

Step 4: Configuring policies

1. Go to **Policy** > **Security Policy**> **Policy**.

2. Click **New** and select **Policy** from the drop-down list.

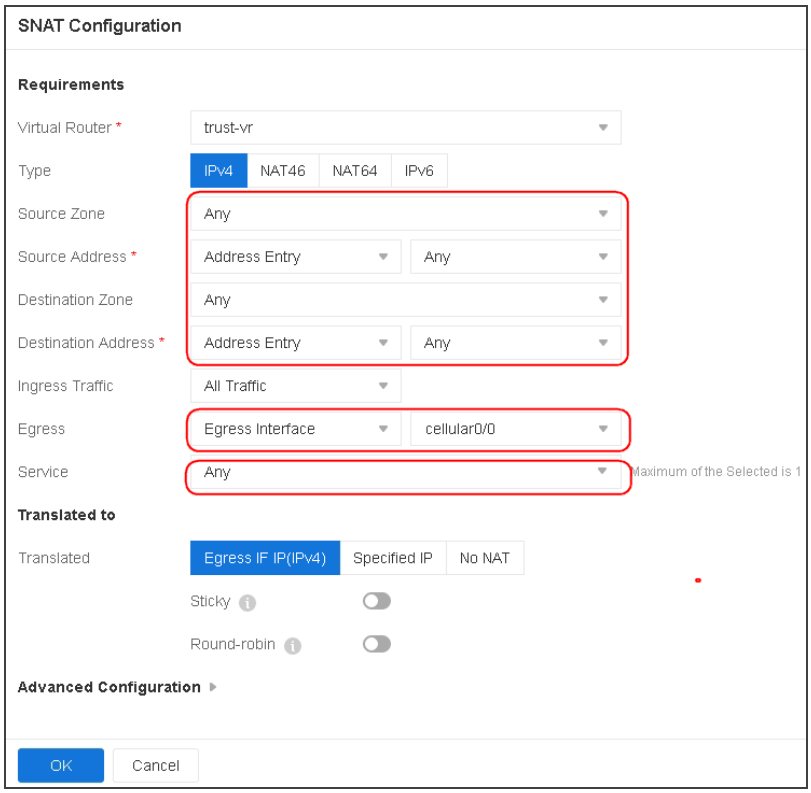


Option	Value
Source Zone	trust
Source Address	Any
Destination Zone	untrust
Destination Address	Any
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

Step 5: Configuring the SNAT Rule

1. Go to **Policy > NAT > SNAT**.

2. Click **New**.



Option	Value
Requirements	
Virtual Router	trust-vr
Source Address	Address Entry, Any
Destination Address	Address Entry, Any
Egress	Egress interface, cellular0/0
Translated to	

Option	Value
Translated	Egress IP
Advanced Configuration	
ID	Automatically assign

Notes: The egress interface should be specified as the Internet interface.

3. Click **OK**.

Step 6: Configuring the IP Address, Gateway, and DNS of Your PC (The IP address must be in the same network segment as ethernet0/1, and the DNS must be specified as the public DNS)

Restoring Factory Settings

Notes: Resetting your device will erase all configurations, including the settings that have been saved. Please be cautious!

To restore the device to the factory default settings, use one of the following ways:

- "Restoring via the CLR Button" on Page 53
- "Restoring via WebUI" on Page 55

Restoring via the CLR Button

To restore the device to the factory default settings via the CLR button, take the following steps:

Model	Step
SG-6000-A7600、SG-6000-A6800、SG-6000-A5860、SG-6000-A5800、SG-6000-A5660、SG-6000-A5600、SG-6000-A5560、SG-6000-A5555、SG-6000-A5500、SG-	1. When the device is working, use a pin to press the CLR button in the pinhole. 2. After a few seconds, the CON port

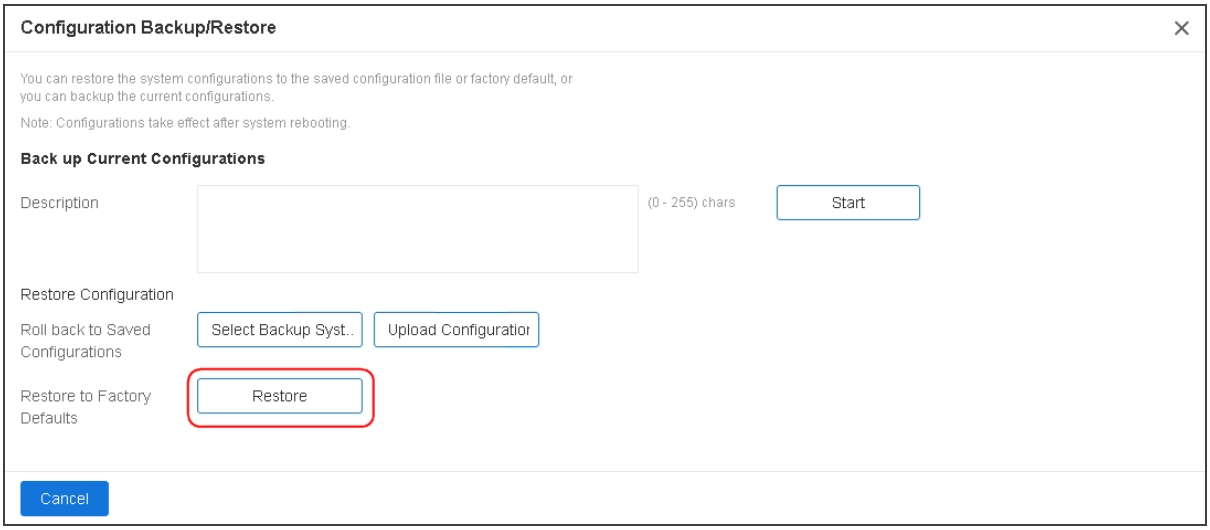
Model	Step
6000-A5260、SG-6000-A5255、SG-6000-A5200、SG-6000-A5160、SG-6000-A5155、SG-6000-A5100、SG-6000-A3815、SG-6000-A3800、SG-6000-A3700、SG-6000-A3615、SG-6000-A3600、SG-6000-A3000、SG-6000-A2815、SG-6000-A2800、SG-6000-A2715、SG-6000-A2700、SG-6000-A2600、SG-6000-A2000、SG-6000-A1100、SG-6000-A1000	prints the message "Clear button is pressed, the machine will power down" and the STA and ALM LEDs turn solid red. After the STA and ALM LEDs turn off, the device will restart. During the startup process, the CON port prints the message "CLR button pressed".
SG-6000-A2205、SG-6000-A1805、SG-6000-A1605、SG-6000-A200、SG-6000-A200W、SG-6000-A200G4、SG-6000-A200WG4	Method 1: 1. Power off the device. 2. Use a pin to press the CLR button in the pinhole; keep pressing and power on the device and the STA LED is green. 3. Keep pressing until the green STA LED starts blinking . System will start to reset itself. Method 2: 1. When the device is working and the STA LED blinking, use a pin to press the CLR button in the pinhole until the STA LED being off and the device rebooting.

Model	Step
	2. Keep pressing until the STA LED turns to solid green. System will start to reset itself.

Restoring via WebUI

To restore the device to factory default settings via WebUI, take the following steps:

1. Go to **System > Configuration File Management>Configuration File List**.
2. Click **Backup Restore**.
3. In the prompt, click **Restore**.



4. Click **OK**.
5. The device will automatically reboot and is restored to factory settings.

General Features

This section introduces the following features:

- Device Management: introduces how to configure password policies, how to back up and restore system configuration, and how to export system debug information.
- Threat Prevention: introduces how to quickly enable threat protections.
- High Availability (HA): introduces how to configure HA.
- Exporting Logs: introduces how to export logs to the log server.

Device Management

This section mainly includes the following aspects:

- Configuring Password Policies: introduces how to configure password policies to enhance system security.
- Backing up and Restoring System Configuration: introduces how to back up the current system configuration and how to restore the system to the backed-up configuration.
- Exporting System Debug Information: introduces how to export system debug information to your local PC.

Configuring Password Policies

You can configure password policies to enhance system security.

Application Scenario

An enterprise firewall device has several administrator accounts. To enhance system security, the enterprise wants to modify the password policy of these administrator accounts. Specific requirements are as follows.

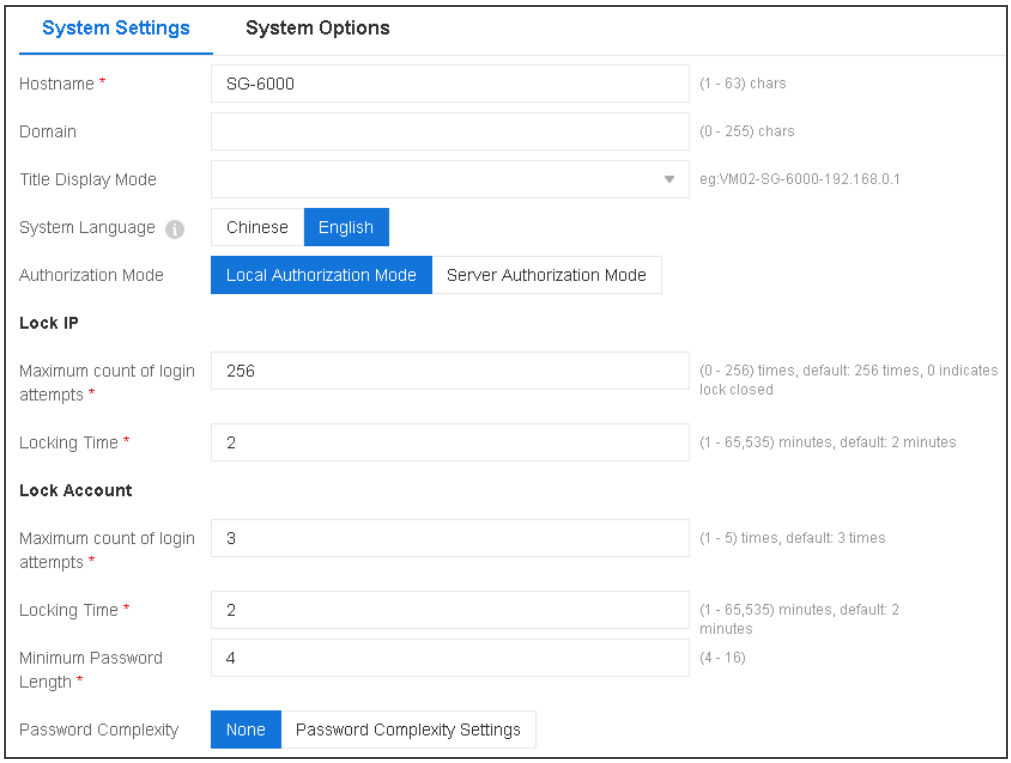
- When an administrator account is created or the password of an existing administrator account is modified, the new password should contain at least 8 characters, including uppercase and lowercase letters, numeric and special characters.
- If the administrator enters the wrong password for three consecutive times at login, this administrator account will be locked out for 60 minutes, during which the account is unable to be logged in.
- The password valid period is 30 days. The account password expires every 30 days. If the password remains unchanged for 30 days, the account will be unable to be logged in.

Configuration Steps:

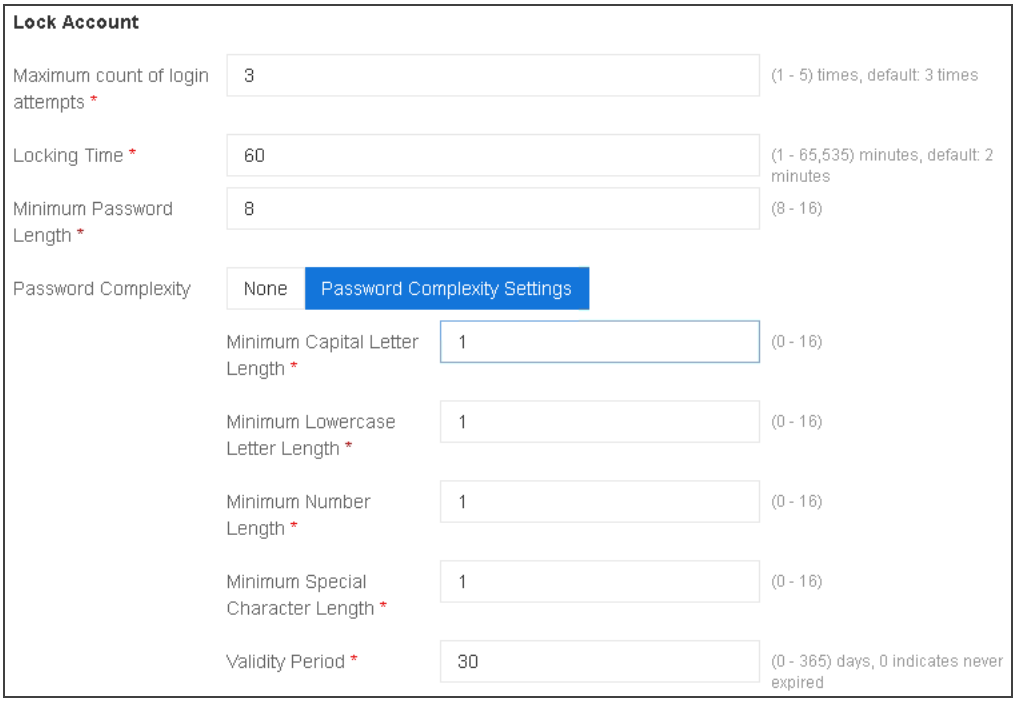
Step 1: Modifying the Password Policy

1. Select **System** > **Device Management** > **Settings & Options**.

2. On the **System Settings** tab, view the current password policy in the **Lock Account** section.



3. Modify the password policy.



In the Lock Account section, configure the new password policy.

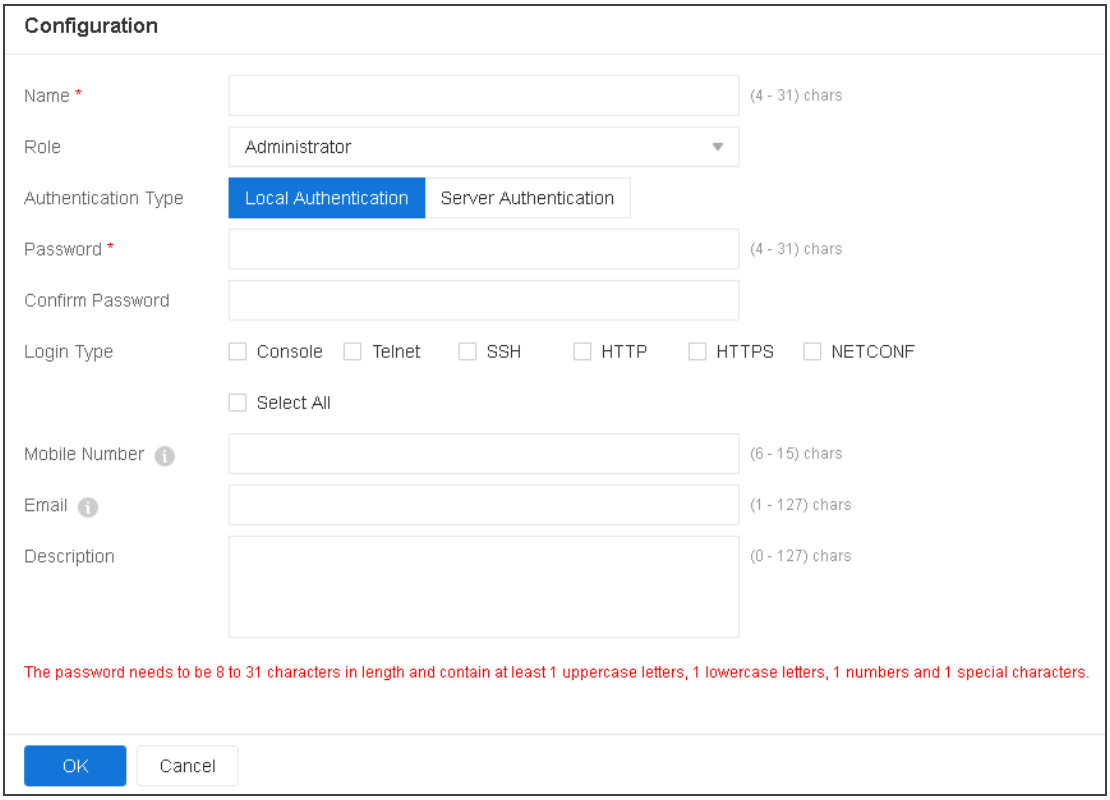
Option	Value
Maximum count of login attempts	3 times
Locking Time	60 minutes
Minimum Password Length	8 characters
Password Complexity	Select **Password Complexity Settings**.
Minimum Capital Letter Length	1 character
Minimum Lowercase Letter Length	1 character
Minimum Number	1 character

Option	Value
Length	
Minimum Special Character Length	1 character
Valid Period	30 days

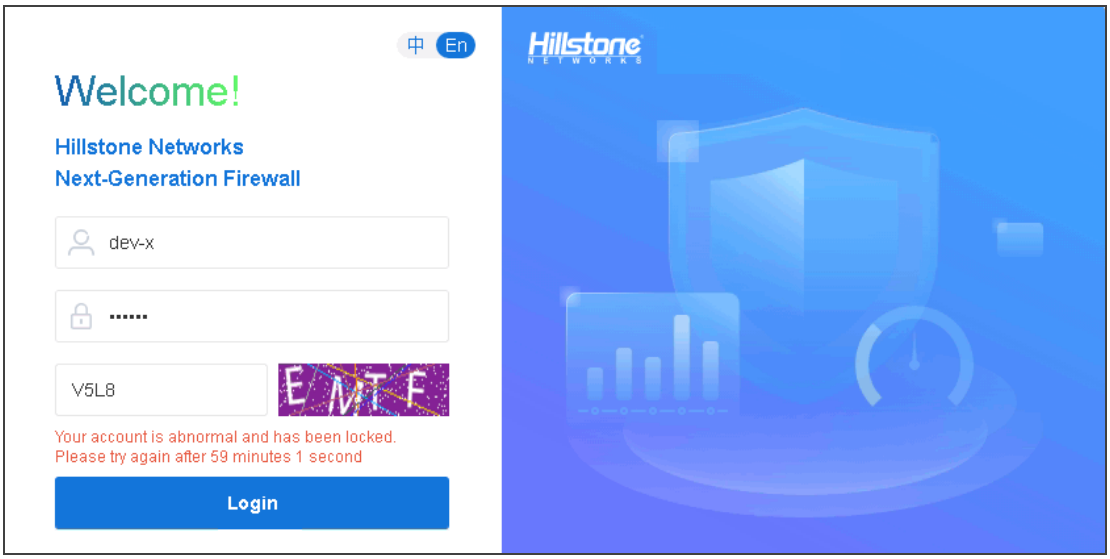
4. Click **OK**.

Step 2: Verifying the Password Policy

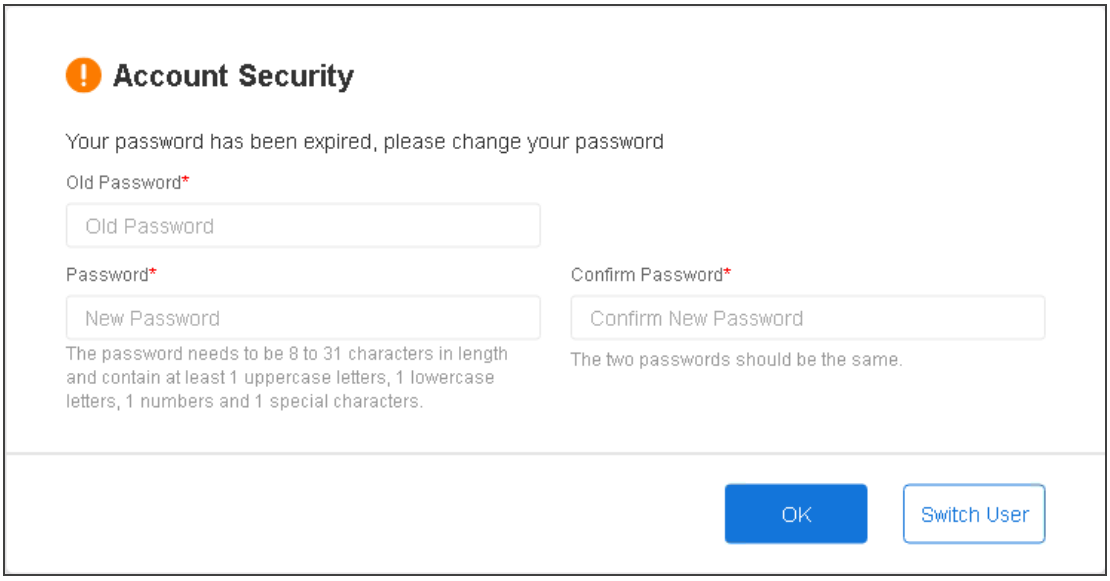
- Select **System** > **Device Management** > **Administrators**. Click **New** or select an existing account and click **Edit**. On the **Configuration** page, new password policy is displayed. When an administrator account is created or the password of an existing administrator account is modified, the new password should meet the new password policy.



- If the administrator enters the wrong password for three consecutive times at login, this administrator account will be locked out. A message will be displayed on the login page, indicating that the account is abnormal and has been locked.



- When the password expires, the system prompts an account security message, indicating that the password has expired and needs to be changed.



Backing up and Restoring System Configuration

You can back up the current system configuration and restore the system to the backed-up configuration.

Application Scenario

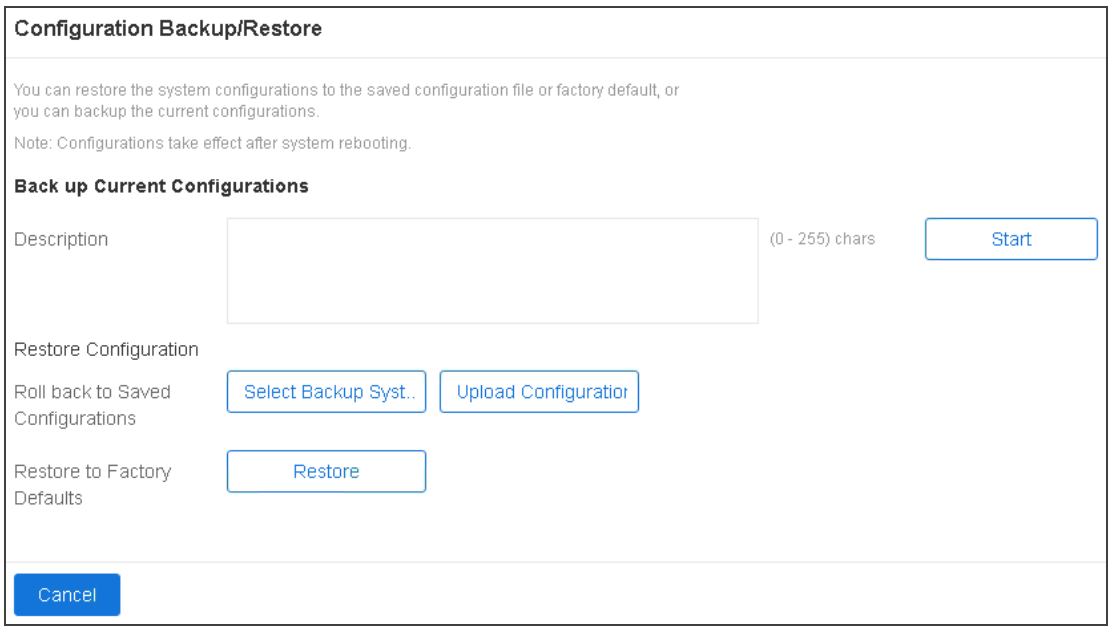
A user needs to upgrade the system version of the firewall. After the upgrade, the user wants to restore the system configuration to the one saved before the upgrade.

Configuration Steps

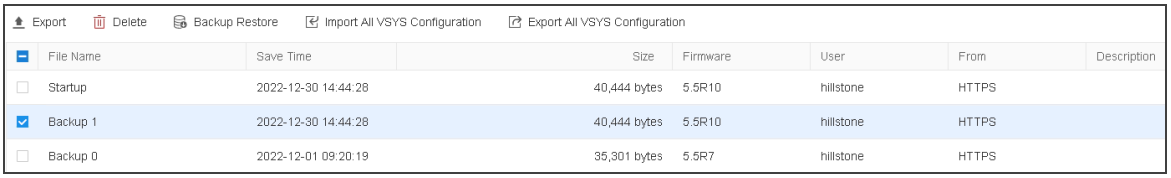
Step 1: Backing Up Current Configuration

Before upgrading the system version, back up the current configuration.

1. Select **System** > **Configuration File Management** > **Configuration File List**.
2. On the **Configuration File List** page, click **Backup Restore** to go to the **Configuration Backup/Restore** panel.
3. Click **Start** and the system will start to save current configuration to the configuration file.



4. When the backup process is finished, the configuration file list is displayed, where the new **Backup 1** configuration file is added.

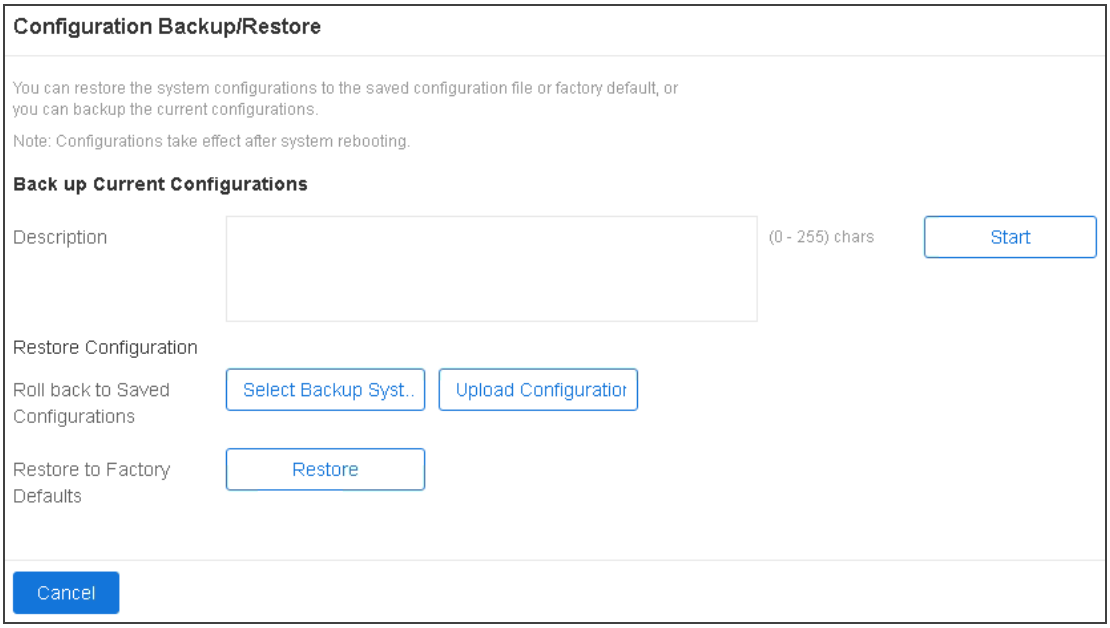


5. (Optional) If needed, select the check box before **Backup 1** and then click **Export** to save the configuration file to your local PC.

Step 2: Restoring to the Configuration Saved Before the Upgrade

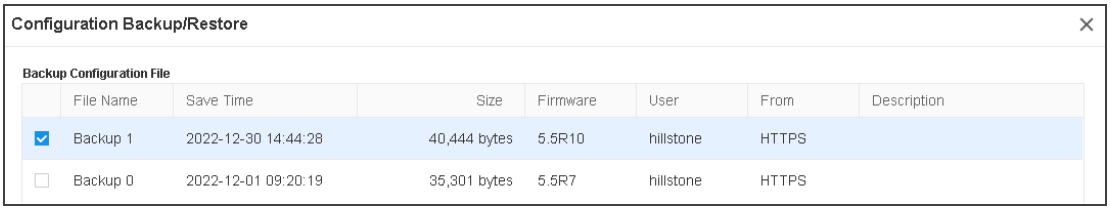
After upgrading the system version, restore the system to the configuration backed up before the upgrade.

1. Select **System** > **Configuration File Management** > **Configuration File List**.
2. On the **Configuration File List** page, click **Backup Restore** to go to the **Configuration Backup/Restore** panel.



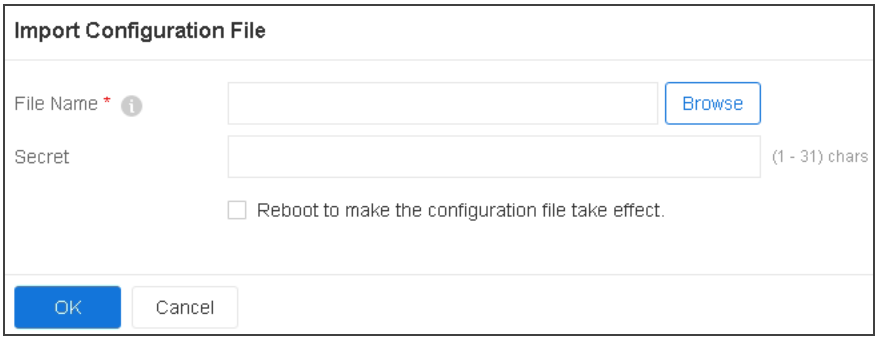
3. Select either of the following methods to restore the system configuration:

- Select the configuration file from the backup configuration file list: Click **Backup System Configuration File** and select **Backup 1**. Click **OK**.



On the reboot prompt, click **OK**. After the device is restarted, the system is restored to the configuration backed up before the upgrade.

- Upload the configuration file: Click **Upload Configuration File**. On the **Import Configuration File** panel, click **Browse** and select the configuration file that needs to be uploaded. To make the configuration take effect immediately, select the check box of **Reboot to make the configuration file take effect**. Click **OK**.



Exporting System Debug Information

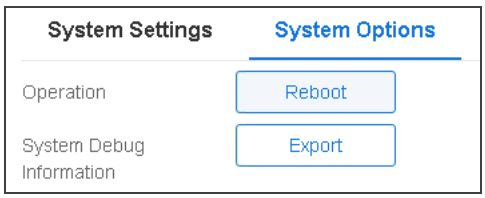
When the device fails, you can export the system debug information to a local PC or forward it to the technical support team to identify the problem.

Application Scenario

A customer's firewall device fails, so the customer wants to export the system debugging file to the technical support team for troubleshooting.

Configuration Steps:

1. Select **System > Device Management> Settings & Options**.
2. Click the **System Options** tab.
3. Click Export to export the tech-support file to your local PC.



4. Open the tech-support file, which contains files such as the coredump file and system logs.
5. Forward the tech-support file to the technical support team to identify the problem.

Threat Prevention

Threat prevention means that the device can detect and block network threats. By configuring the threat prevention function, Hillstone devices can defend network attacks and reduce losses of the Intranet.

Threat protections include:

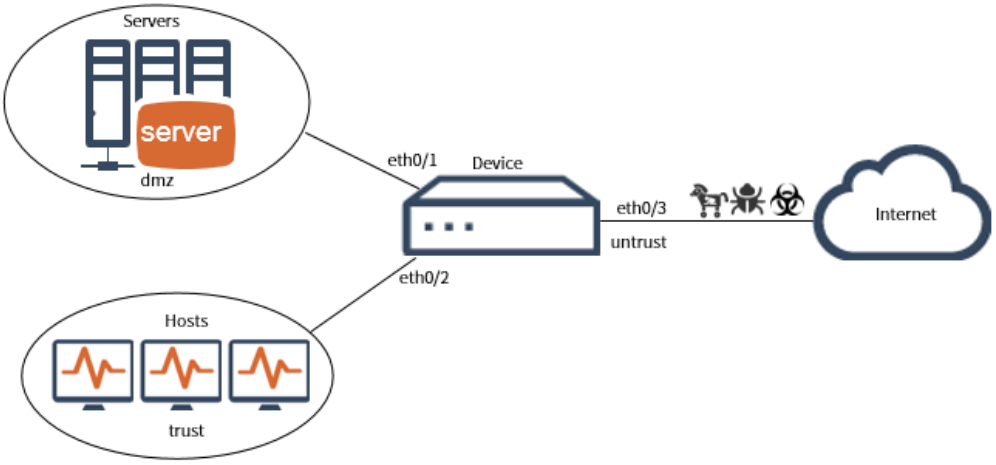
- Anti Virus: It can detect common file types and protocol types which are most likely to carry the virus, and protect the network from them. Hillstone devices can detect protocol types of HTTP, SMTP, POP3, IMAP4, FTP, and SMB and the file types of archives (including GZIP, BZIP2, TAR, ZIP and RAR-compressed archives), PE, HTML, MAIL, RIFF, ELF, PDF, MS OFFICE, Raw Data, and Others. **Others** means scanning other files, including GIF, BMP, PNG, JPEG, FWS, CWS, RTF, MPEG, Ogg, MP3, wma, WMV, ASF, RM, etc.
- Intrusion Prevention: It can detect and protect mainstream application layer protocols (DNS, FTP, HTTP, POP3, SMTP, TELNET, MYSQL, MSSQL, ORACLE, NETBIOS, etc.) against intrusion attacks, web-based attacks, and common Trojan attacks.
- Attack Defense: It can detect various types of network attacks and take appropriate actions to protect the Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.
- Sandbox Protection: It can executes suspicious files in the virtual environment, collect dynamic behaviors of suspicious files, analyze these dynamic behaviors, and determine the validity of files based on the analysis results.
- Anti-Spam: It can filter the mails transmitted by SMTP and POP3 protocol through the cloud server, and discover the mail threats.
- Botnet Prevention: It can detect botnet host in the Intranet timely, and locate and take corresponding actions according to the configuration, so as to avoid further threat attacks.

The threat prevention function may vary in different platforms. Please refer to the system's actual page.

Application Scenario

This section uses anti-virus, IPS, attack defense, and botnet prevention as the example to introduce how to quickly enable these common threat prevention functions, detect threats against the traffic passing through the firewall, and block attacks, thus protecting enterprise information systems and networks from attacks.

The networking environment is shown in the following picture. The device is deployed at the Intranet exit. Interface ethernet0/1 belongs to dmz zone and is connected to the Intranet server farm. Interface ethernet0/2 belongs to the trust zone and is connected to Intranet employees. Interface ethernet0/3 belongs to the untrust zone and is connected to the Internet.



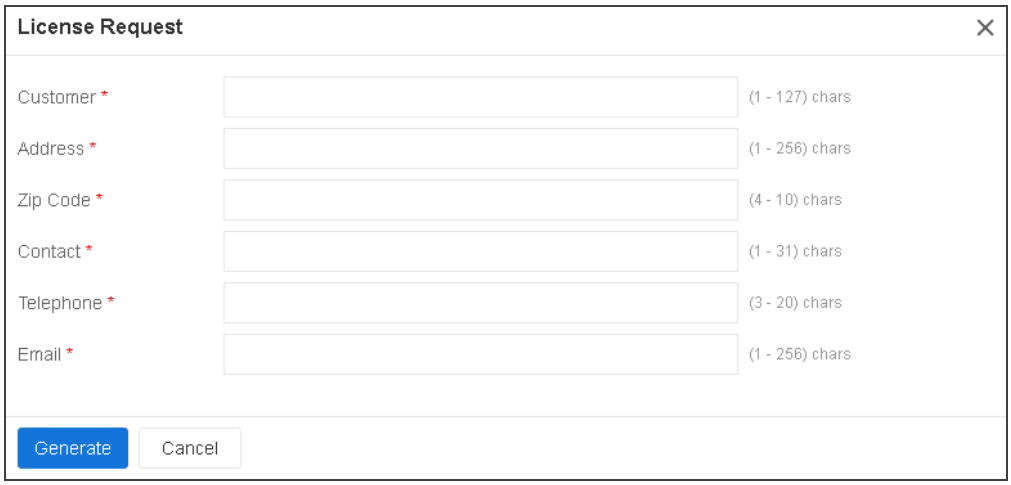
Configuration Steps

Step 1: Installing Licenses

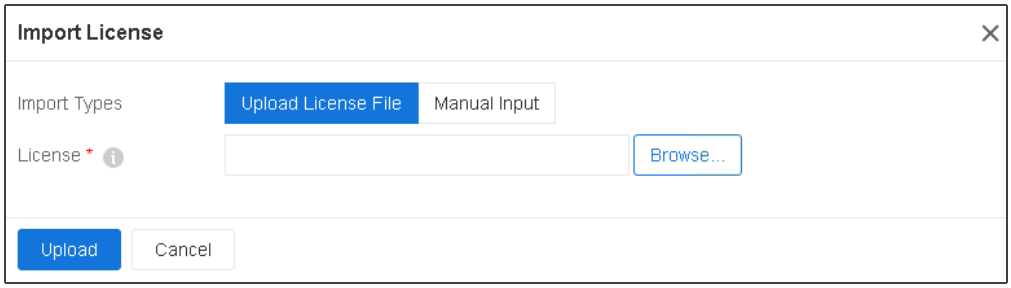
Anti-virus, IPS, and botnet prevention are controlled by licenses. To use these functions, apply and install corresponding licenses.

1. Select **System** > **License**. Click **Apply For**. On the **License Request** panel, fill in the application information. Click **Generate**, and then a bunch of code appears. Send the to your sales

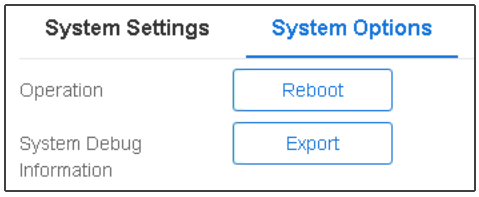
contact. The sales person will issue the license and send the license code back to you.



2. Select **System** > **License** , and click **Import**. On the **Import License** page, Select **Upload License File** and click **Browse** to select the license file and then click **OK** . Repeat this step to upload anti-virus (AV) license, IPS license, and botnet prevention license.



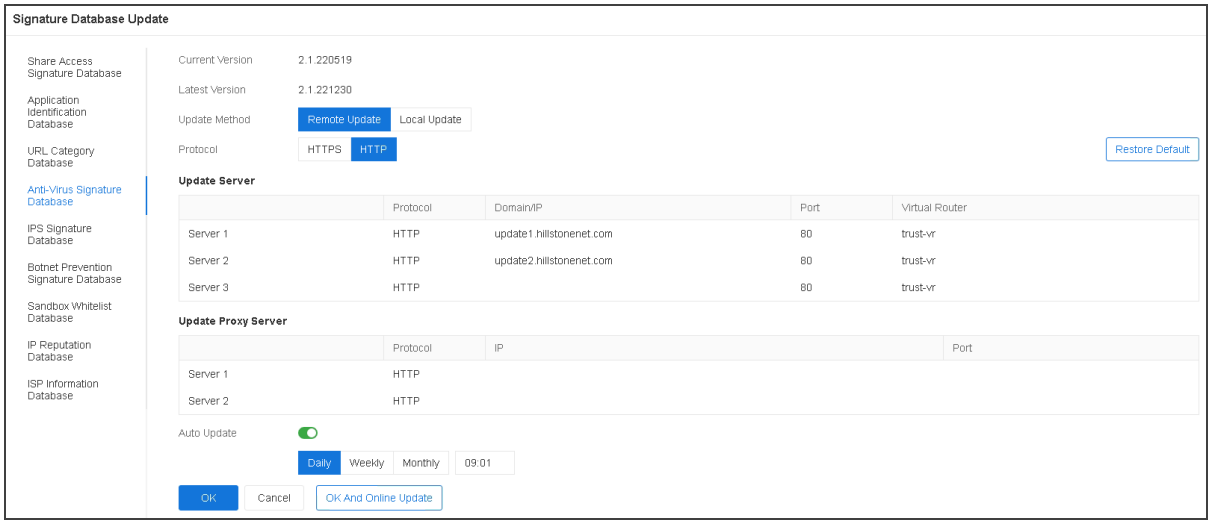
3. Select System > Device Management > Settings & Options. On the System Options tab, click **Reboot**, and select **Yes** in the prompt. Installed license(s) will take effect after the system restarts.



Step 2: Upgrading the Signature Database

If you use the anti-virus, IPS, botnet prevention for the first time, update the signature databases corresponding to each function - the AV signature database, IPS signature database, and botnet prevention signature database.

Select **System** > **Upgrade Management** > **Signature Database Update**. In the Anti-Virus Signature Database section, click **OK and Online Update** to update the AV signature database right now. Repeat this step to update IPS signature database and botnet prevention signature database.



Notes: To ensure that the device can connect to the default update server, configure the DNS server for the device before the update.

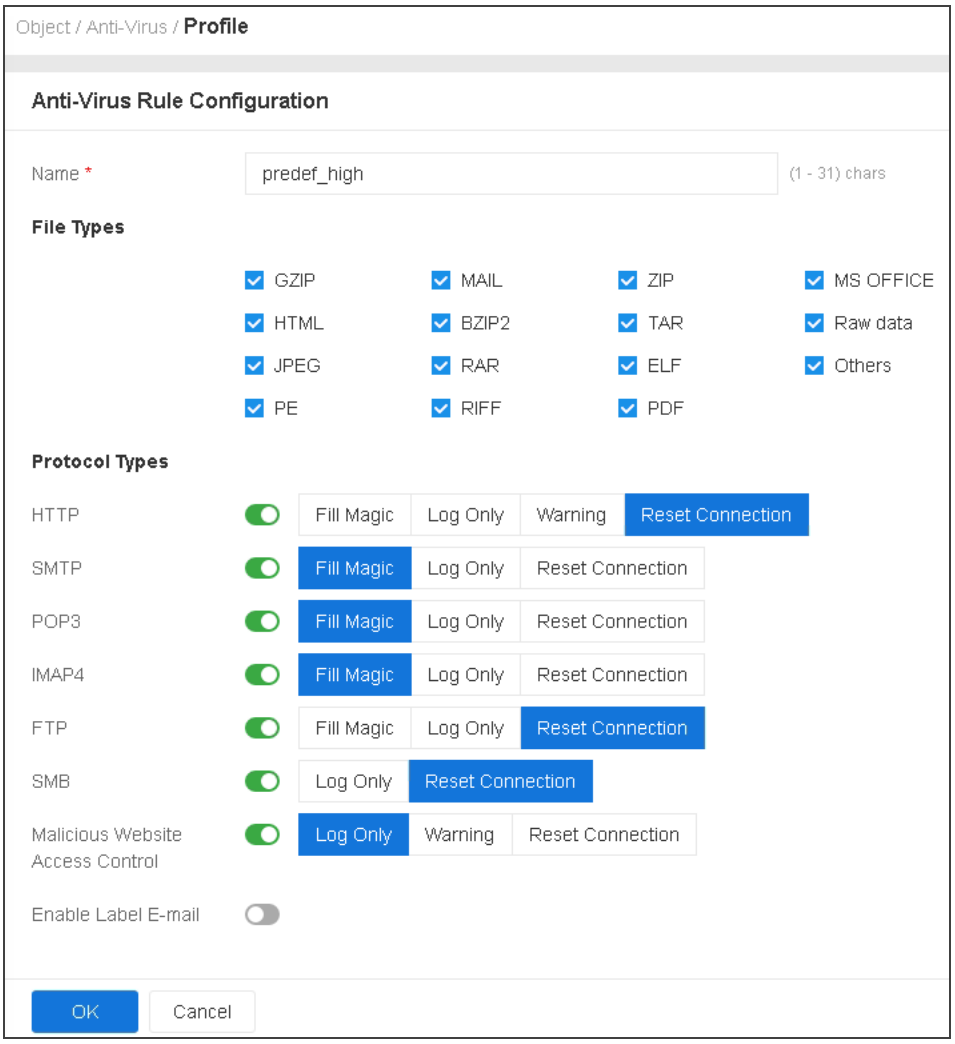
Step 3: Creating a Threat Prevention Rules

- Creating an Anti-Virus Rule

  You can use the predefined anti-virus rule or create customized rules. Select **Object** > **Anti-Virus** > **Profile**. Click **New** to customize an AV rule.

  This example uses the predefined " predef_high" AV rule. The rule is the strictest with all file types and protocol types scanned. The protection action for mail transfer protocols is **Fill**

Magic. The protection action for other protocols is **Reset Connection**.

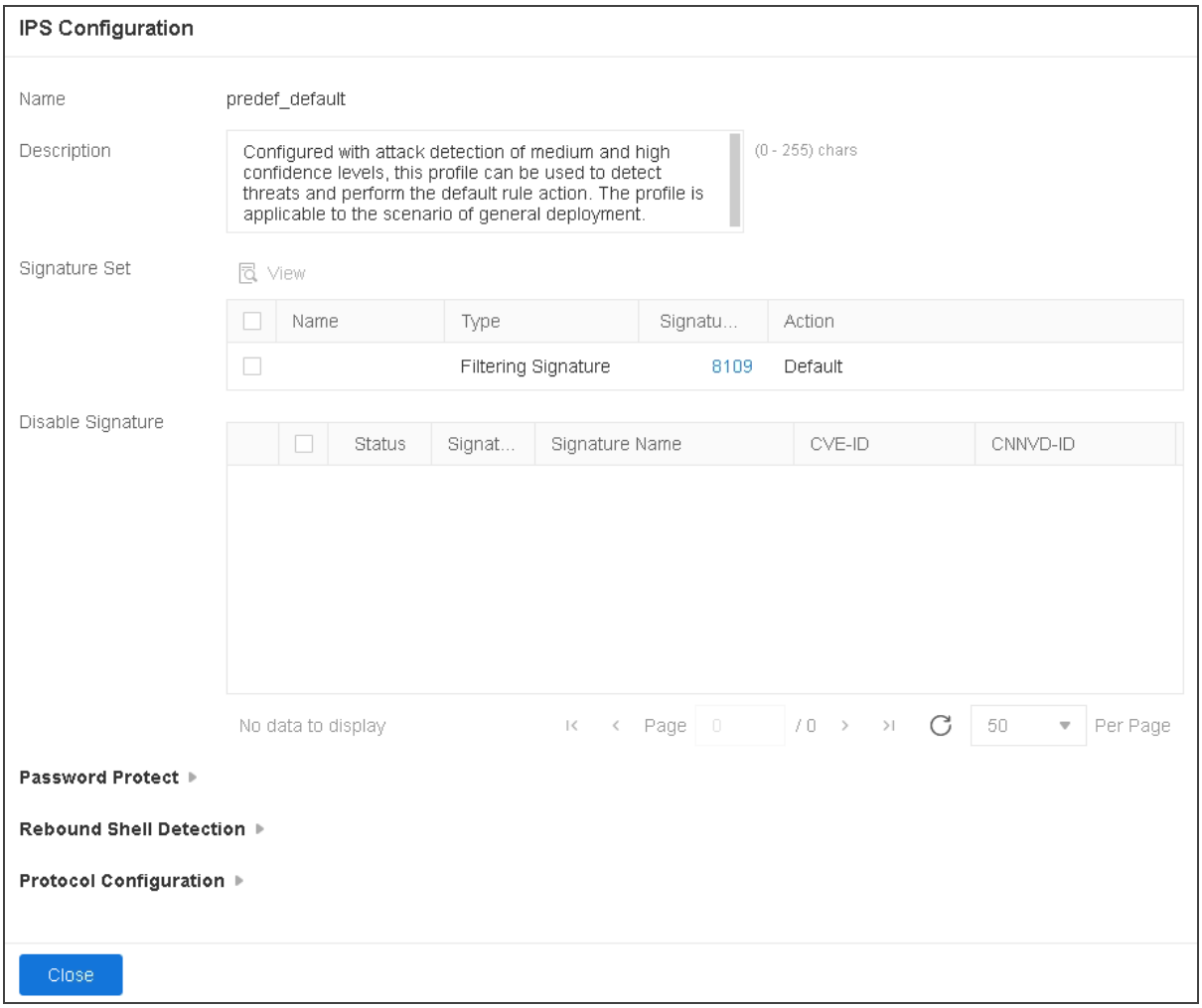


- Creating an IPS Rule

  You can use the predefined IPS rule or create customized rules. Select **Object** > **Intrusion Prevention System**> **Profile**. Click **New** to customize an IPS rule.

  This example uses the predefined "predef_default" IPS rule, where attack detections of medium and high confidence levels are included. This rule profile can be used to detect

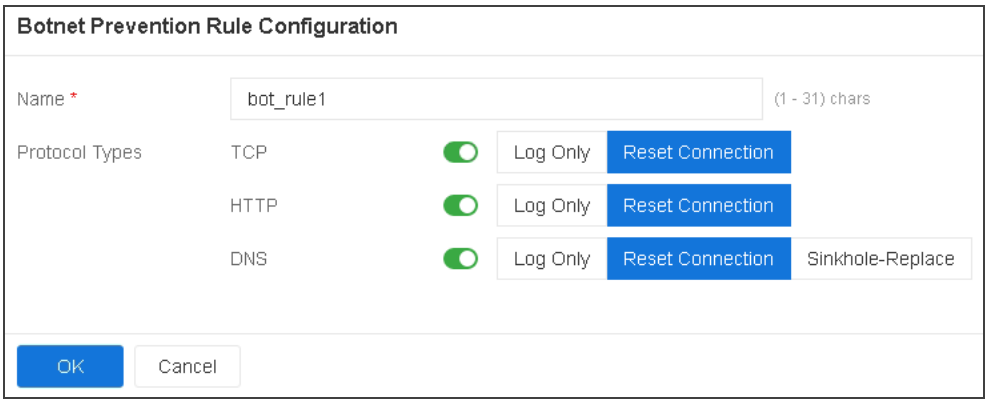
threats and perform the default rule action.



- Creating a Botnet Prevention Rule

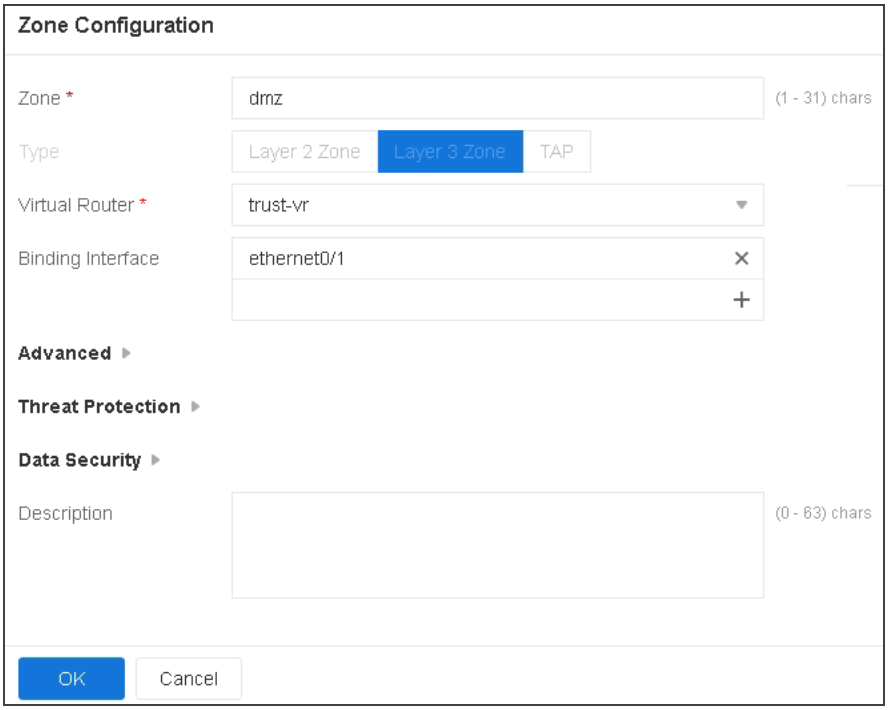
  Select **Object** > **Botnet Prevention**> **Profile**. Click **New** to create a botnet prevention profile named bot_rule1. In this profile, the protocol types are TCP, HTTP, and DNS and the pro-

tection action for these protocols is **Reset Connection**.



Step 4: Binding Intranet and Internet Interfaces to Corresponding Zones

1. Bind the Intranet interface ethernet0/1 to Zone "dmz". Select **Network** > **Zone**. Select **dmz** and click **Edit**. On the **Zone Configuration** page, select ethernet0/1 from the **Binding Interface** drop-down list.



2. Use the same method to bind Intranet interface ethernet0/2 to Zone "trust".

3. Use the same method to bind Internet interface ethernet0/3 to Zone "untrust".

Step 5: Enabling the Attack Defense

The system supports zone-based attack defense function.

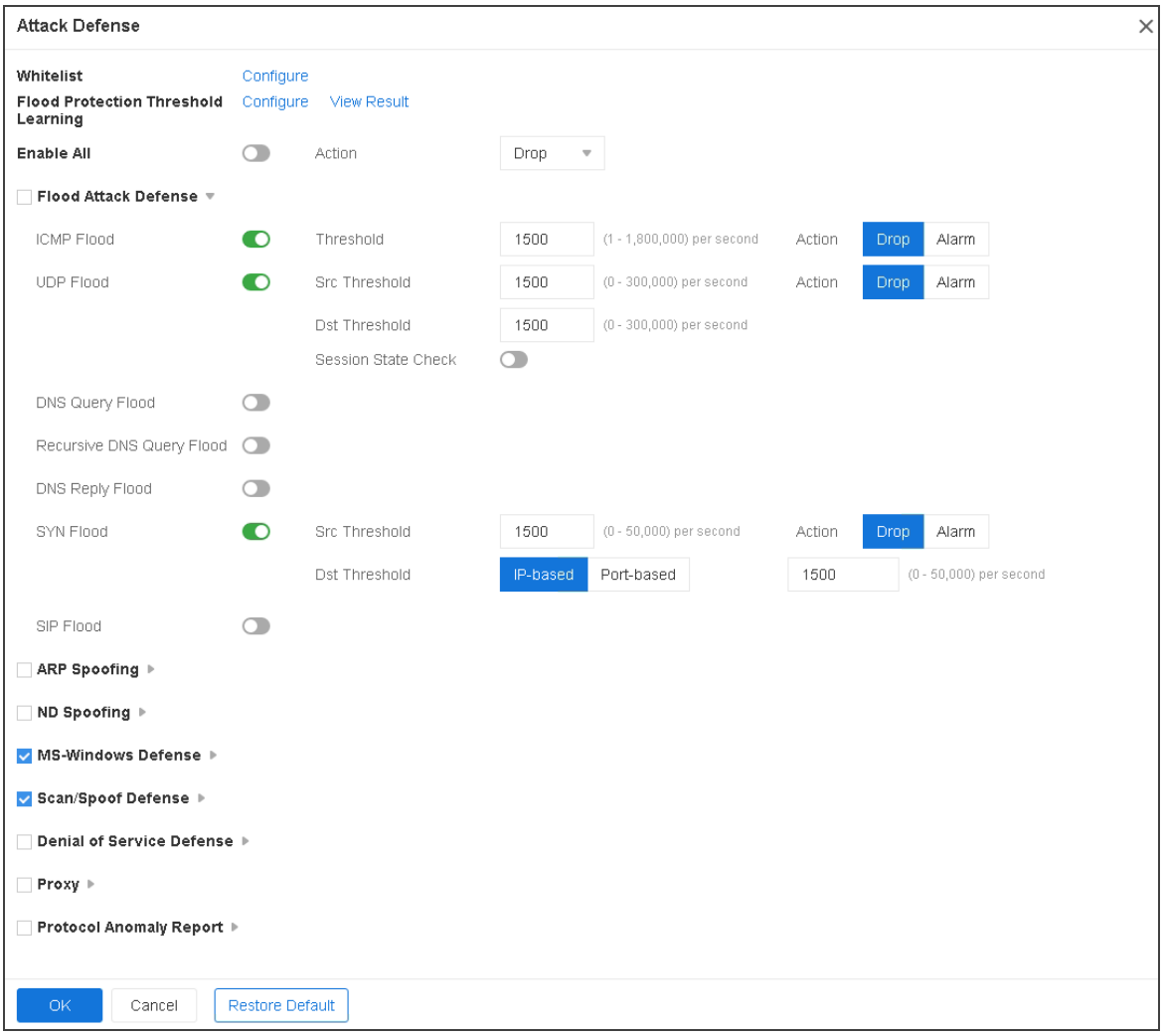
1. Select **Network** > **Zone** and double click "untrust".

2. Expand the **Threat Protection** section and click the button to enable the zone-based attack defense(AD) function.



You can use the default AD configuration or click **Configure** to set customized configuration. In this example, the default attack defense configuration is used, that is, ICMP flood attack defense, UDP flood attack defense, SYN flood attack defense, MS-Windows

defense, and scan/spoof defense are all enabled and the action is **Drop**.



Step 6: Creating a Policy and Enabling Anti-Virus, IPS, and Botnet Prevention

To allow the Internet to access enterprise server farm, configure the untrust-dmz policy, and enable anti-virus and IPS, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.

2. Click **New** and select **Policy** from the drop-down list.

Option	Value
Source Zone	untrust
Source Address	Any
Destination Zone	dmz
Destination Address	Any
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

   Expand the Protection section and configure the following options.

Option	Value
Anti-Virus	Click the button to enable the anti-virus function and select pre-def_high from the drop-down list.
IPS	Click the button to enable the IPS function and select predef_ default from the drop-down list.

3. Click **OK**.

To allow enterprise offices to access the Internet, configure the trust-untrust policy, and enable botnet prevention, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.

2. Click **New** and select **Policy** from the drop-down list.

Option	Value
Source Zone	trust
Source Address	Any
Destination Zone	untrust
Destination Address	Any
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

Expand the Protection section and configure the following options.

Option	Value
Botnet Pre-vention	Click the button to enable the IPS function and select bot_rule1 from the drop-down list.

3. Click **OK**.

To allow enterprise offices to access the enterprise server farm, configure the trust-dmz policy, and enable anti-virus, IPS, and botnet prevention, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.

2. Click **New** and select **Policy** from the drop-down list.

Option	Value
Source Zone	trust
Source Address	Any

Option	Value
Destination Zone	dmz
Destination Address	Any
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

Expand the Protection section and configure the following options.

Option	Value
Anti-Virus	Click the button to enable anti-virus and select predef_high from the drop-down list.
IPS	Click the button to enable the IPS function and select predef_ default from the drop-down list.
Botnet Pre-vention	Click the button to enable the IPS function and select bot_rule1 from the drop-down list.

3. Click **OK**.

Step 7: Viewing Detection Results

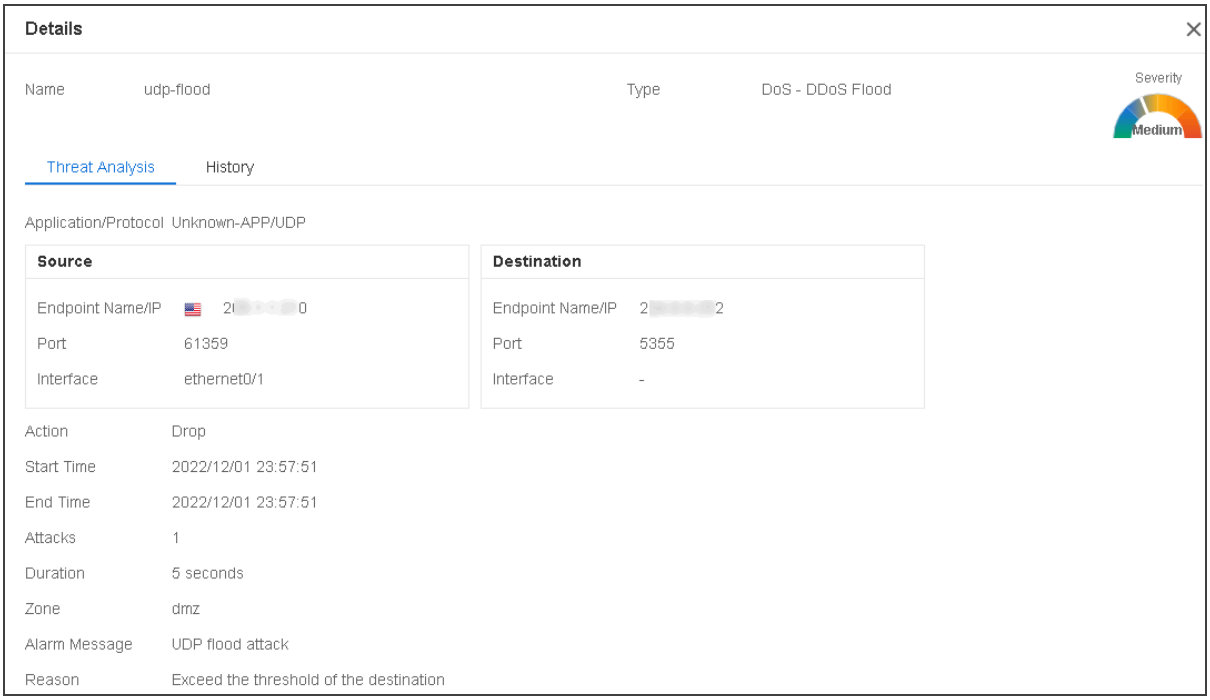
The following example introduces how to view the detection results of attack defense.

View iCenter:

1. Select **iCenter** > **Threat**. Click **Filter** to add filtering conditions.

    - Detection Engine: Attack Defense

2. After adding the filtering condition, you will see threat event of Attack Defense. Click the threat name to view its details.

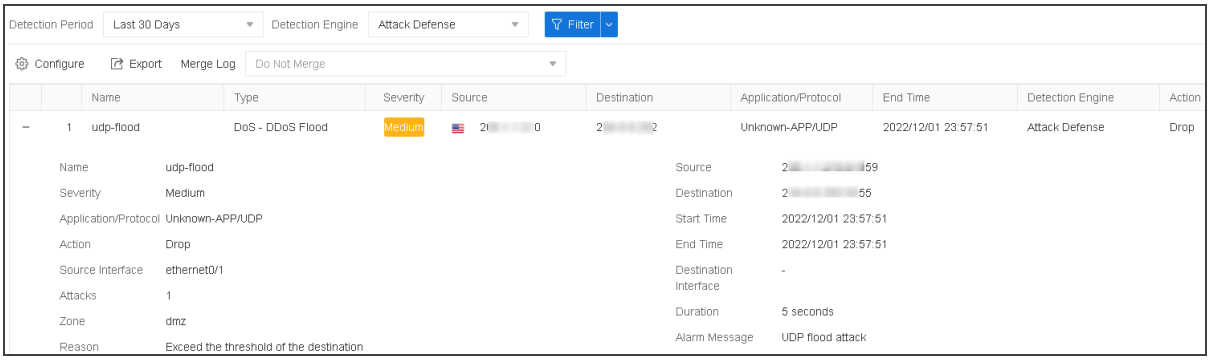


Viewing Threat Logs:

1. Select **Monitor** > **Log** > **Threat Log**. Click **Filter** to add filtering conditions.

    - Detection Engine: Attack Defense

2. After adding the filtering condition, you will see threat logs of Attack Defense. Click + before the threat name to view its details.



High Availability (HA)

HA, the abbreviation for High Availability, provides a fail-over solution for communications lines or device failure to ensure the smooth communication and effectively improve the reliability of the network. The system supports the following two HA modes:

- Active-Passive (A/P) mode: In the HA cluster, configure two devices to form an HA group, with one device acting as a primary device and the other acting as its backup device. The primary device is active, forwards packets, and meanwhile synchronizes all of its network and configuration information and current session information to the backup device. When the primary device fails, the backup device will be promoted to primary and takes over its work to forward packets. This A/P mode is redundant, and features a simple network structure for you to maintain and manage.
- Peer Active-Active (A/A) mode: the Peer A/A mode is an HA Active-Active mode. In the Peer A/A mode, two devices are both active, perform their own tasks simultaneously, and monitor the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously. In the Peer A/A mode, only the device at the active status can send/receive packets. The device at the disabled status can make two devices have the same configuration information but its interfaces do not send/receive any packets. The Peer A/A mode is more flexible and is suitable for the deployment in the asymmetric routing environment.

Requirements

HA, the abbreviation for High Availability, provides a fail-over solution for communications lines or device failure to ensure the smooth communication and effectively improve the reliability of the network.

To implement the HA function, you need to configure the two devices as HA clusters with identical settings for the following:

- Hardware platform
- Firmware version
- VSYS （enable VSYS on two devices that are installed with VSYS license or not use VSYS on both devices)
- Virtual Router (enable VR simultaneously on two devices or not use VR on both devices)

When one device is not available or cannot handle the request from the client properly, the request will be promptly directed to the other device that works normally, thus ensuring uninterrupted network communication and greatly improving the reliability of communications.

The configuration of HA clusters is not affected if certain functions, such as AV, are not consistent on the two HA devices. In this scenario, the system sends an alarm showing that certain settings on the two devices are not consistent. It indicates that when the master device fails, the backup device may have problems taking over its work. Settings that cause the above scenario include but are not limited to the below ones:

- enable or disable Antivirus, IPS, URL DB, Perimeter Traffic Filtering, Threat Prevention, Botnet C&C Prevention, Sandbox, IoT Monitor, and Antispam.
- install or not install licenses such as Antivirus License, IPS License, URL DB License, PTF License, Threat Prevention License, Antispam License, Botnet Prevention License, IoT Monitor License, Twin-mode License, Cloud Sandbox Prevention License, Signature Database Application License, and QoS/iQoS License.

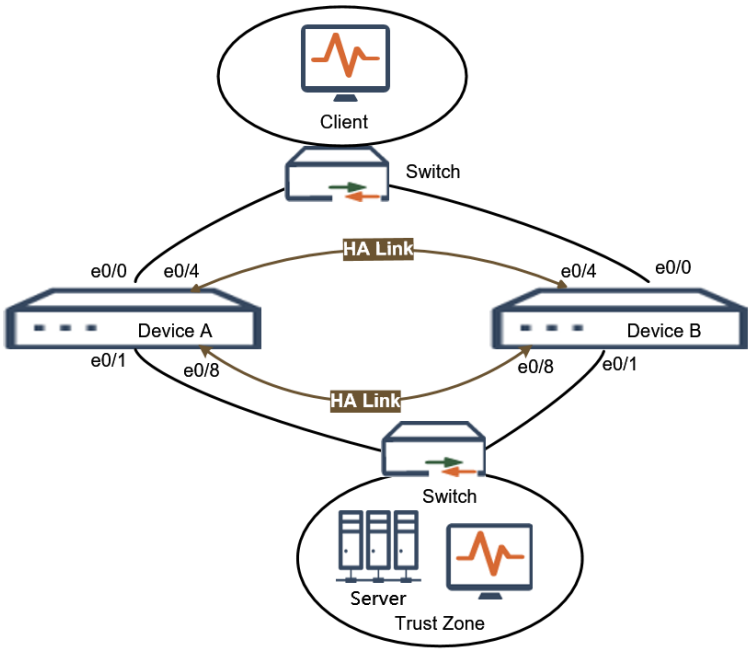
It is suggested to concern on the alarms when the above functions are not consistent on the two HA devices.

Application Scenario

This example introduces how to configure two devices working under Active-Passive mode to provide high availability for the protected network.

As shown in the following tropology, the two devices in HA AP mode are Device A and Device B. After the configuration, Device A is selected as the master device to forward traffic. Device B

is the backup device. Device A synchronizes its configuration and status to backup Device B. When the active Device A is faulty and cannot forward traffic, the backup Device B switches to the master device and continues to forward traffic without affecting user communication.



Configuration Steps

Step 1: Configuring the Track Object. Each device monitors eth0 respectively.

Device A

1. Select **Object** > **Track Object**.
2. Click **New**.



Option	Value
Name	track1
Threshold	255
HA sync	Disabled
Track Type	Select **Interface**, and click **Add**. In the prompt, select ethernet0/0, and specify weight as 255.

3. Click **OK**.

Device B

1. Select **Object** > **Track Object**.
2. Click **New**.



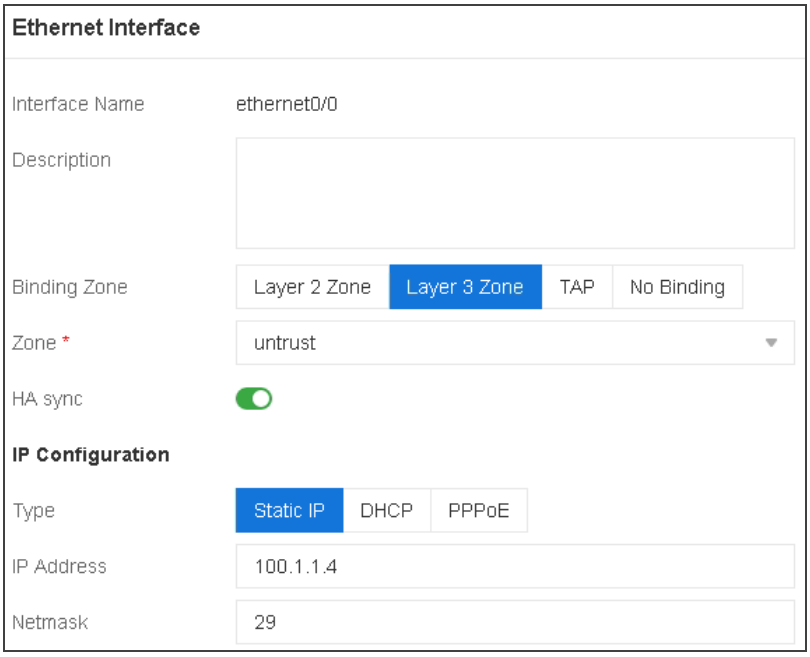
Option	Value
Name	track1
Threshold	255
HA sync	Disabled
Track Type	Select **Interface**, and click **Add**. In the prompt, select ethernet0/0, and specify weight as 255.

3. Click **OK**.

Step 2: Configuring Device A's Interface and Policy

- Configuring ethernet0/0

1. Select **Network > Interface**.
2. Double click "ethernet0/0".

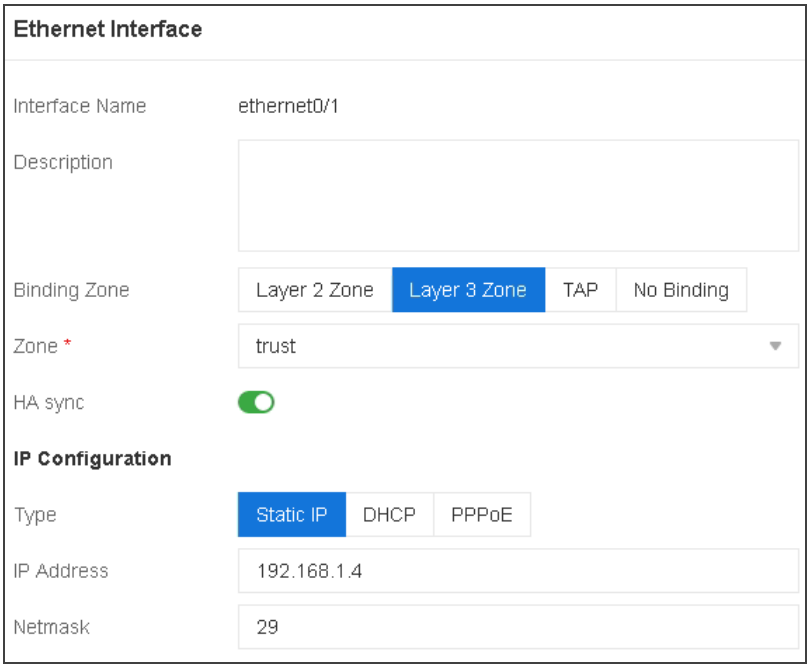


Option	Value
Binding Zone	Layer 3 Zone
Zone	untrust
HA sync	Enable
Type	Static IP
IP Address	100.1.1.4
Netmask	29

3. Click **OK**.

- Configuring ethernet0/1

1. Select **Network > Interface**.
2. Double click "ethernet0/1".



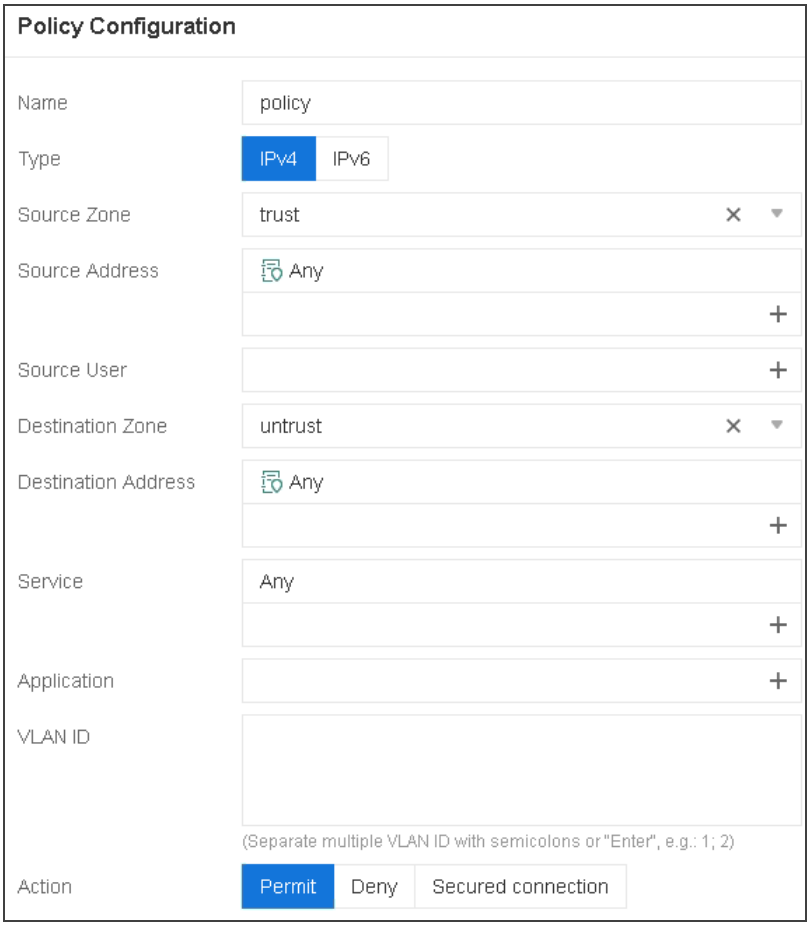
Option	Value
Binding Zone	Layer 3 Zone
Zone	trust
HA sync	Enable
Type	Static IP
IP Address	192.168.1.4
Netmask	29

3. Click **OK**.

- Configuring the Security Policy

1. Select **Policy > Security Policy > Policy**.

2. Click **New** and select **Policy** from the drop-down list.



Option	Value
Name	policy
Source Zone	trust
Source Address	Any
Destination	untrust

Option	Value
Zone	
Destination Address	Any
Service	Any
Action	Permit

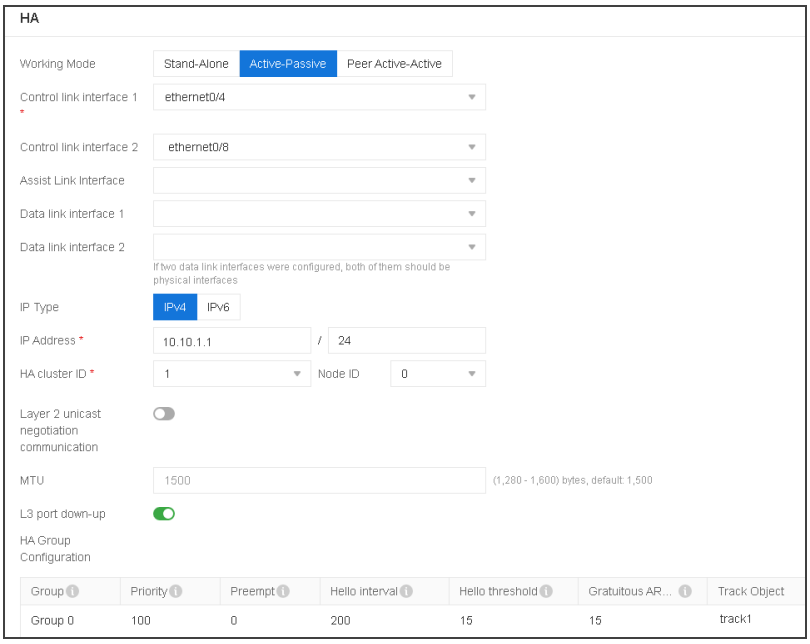
3. Click **OK**.

Step 3: Configuring HA function

Device A

1. Select **System > HA**.

2. For **Working Mode**, select **Active-Passive**.



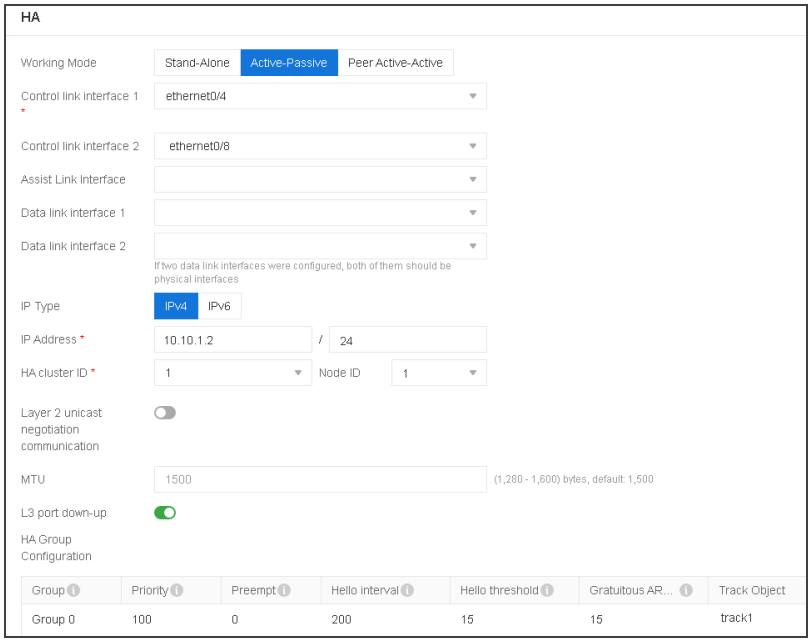
Option	Value
Control link	ethernet0/4

Option	Value
interface 1	
Control link interface 2	ethernet0/8
IP Address	10.10.1.1/24
HA cluster ID	1
Node ID	0
HA Group Configuration	Enter 10 for **Priority** and select **track1** for **Track Object**.

3. Click **OK**.

Device B

1. Select **System > HA**.
2. For **Working Mode**, select **Active-Passive**.



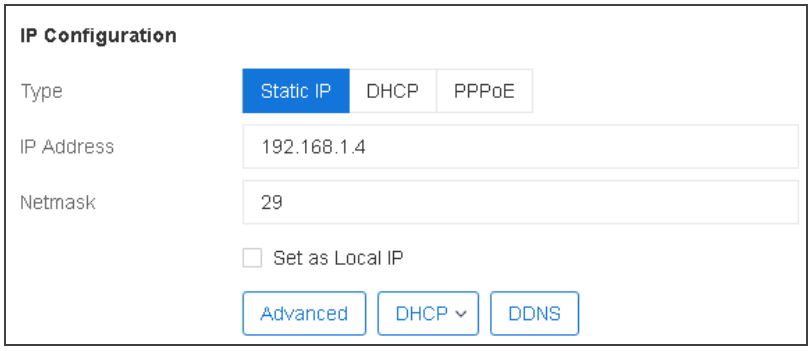
Option	Value
Control link interface 1	ethernet0/4
Control link interface 2	ethernet0/8
IP Address	10.10.1.2/24
HA cluster ID	1
Node ID	1
HA Group Configuration	Enter 100 for **Priority** and select **track1** for **Track Object**.

3. Click **OK**.

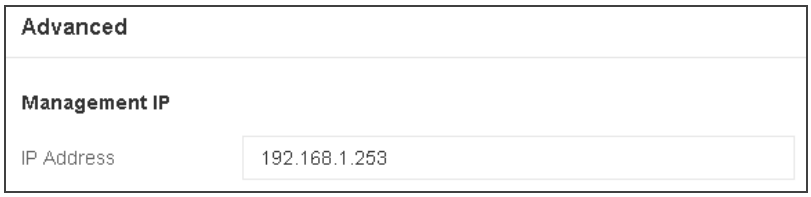
Step 4: Configuring the Management IP of Master and Backup Devices After Synchronization

Device A

1. Select **Network > Interface**.
2. Double click ethernet0/1.
3. On the **Ethernet Interface** page, click **Advanced** in the **IP Configuration** section.



4. On the **Advanced** page, in the **Management IP** section, specify the **IP Address** as 192.168.1.253.

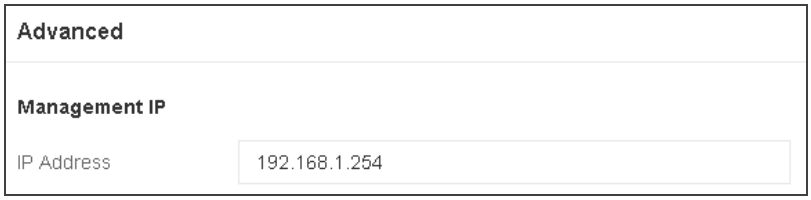


5. Click **OK**.

Device B

1. Select **Network > Interface**.
2. Double click ethernet0/1.
3. On the **Ethernet Interface** page, click **Advanced** in the **IP Configuration** section.

4. On the **Advanced** page, in the **Management IP** section, specify the **IP Address** as 192.168.1.254.



5. Click **OK**.

Step 5: Results

After configuration, select **System > System and Signature Database**. In the **System Information** Section, **HA State** shows the device's HA status.

Device A

- HA State: Master



Device B

- HA State: Backup

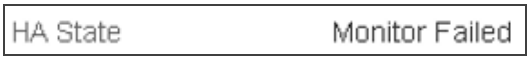


When Device A fails to forward traffic or its eth0/0 is disconnected, Device B will turn to Active and starts forwarding without interrupting protected network.

Select **System > System and Signature Database**. In the **System Information** Section, **HA State** shows the device's HA status.

Device A

- HA State: Monitor Failed



Device B

- HA State: Master

HA State	Master

Exporting Logs

The system supports multiple log types and you can export logs to different destinations. You are allowed to export logs to the following destinations. You can specify the destination as needed.

- Console - Export logs to the Console.
- Terminal- Export logs to Telnet or SSH terminal。
- Cache - Export logs to cache.
- File - Export logs to a file.
- Log Server - Export logs to UNIX or Windows Syslog Server。
- Email Address- Export logs to the specified email address.
- Database - Export logs to the local database, which resides in storage devices, including SD memory cards and USB flash drives and expansion hard drives.
- SMS - Export logs to specified mobile phone as an SMS.

Application Scenario

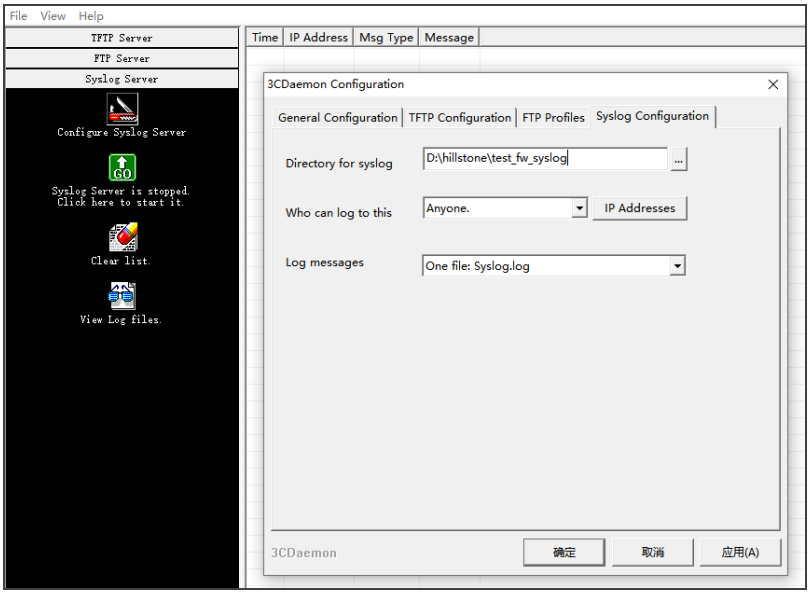
A user needs to view the NAT logs of the firewall deployed at the Intranet exit and the NAT logs of the firewall should be exported to the log server in plaintext.

Configuration Steps

Step 1: Configuring the Log Server on PC

1. Install the log server software on the PC that needs to receive logs. Take 3CDaemon as an example.
2. When the installation is completed, open 3CDaemon.
3. Click **Syslog Server** and then click **Configure Syslog Server**.

4. In the **3CDaemon Configuration** dialogue box, configure the directory for storing the Syslog file, allowed log senders, and the log file name.

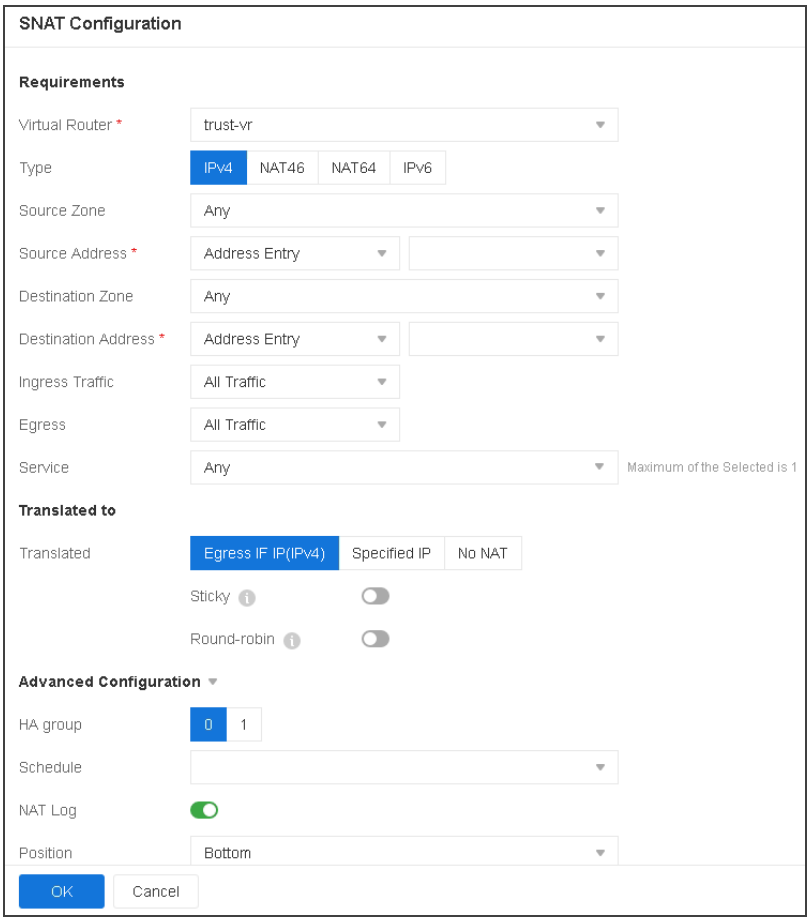


Step 2: Configuring the Export of NAT Logs

To enable the NAT log function of the NAT rule, take the following steps:

1. Select **Policy > NAT > SNAT/DNAT**。
2. Enable NAT Log for each NAT rule. Take the SNAT rule as an example. On the **SNAT Configuration** page, go to **Advanced Configuratio**n section, and click the enable button

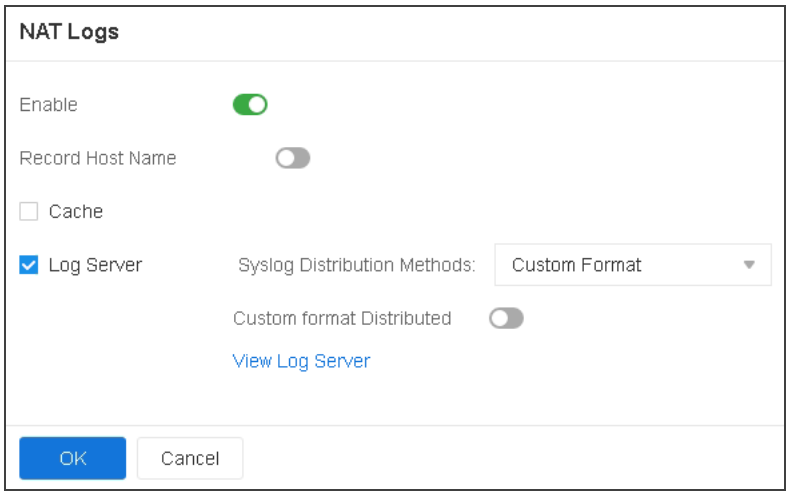
behind **NAT Log**.



To enable the NAT log function of the device, take the following steps:

1. Select **Monitor** > **Log** > **NAT Log**.

2. Click **Configure** to go to the **NAT Logs** panel.



Option	Value
Enable	Click the button to enable the NAT log function.
Log Server	Click the check box of **Log Server** and select **Custom Format** from the **Syslog Distribution Methods** drop-down list.

3. Click **OK**.

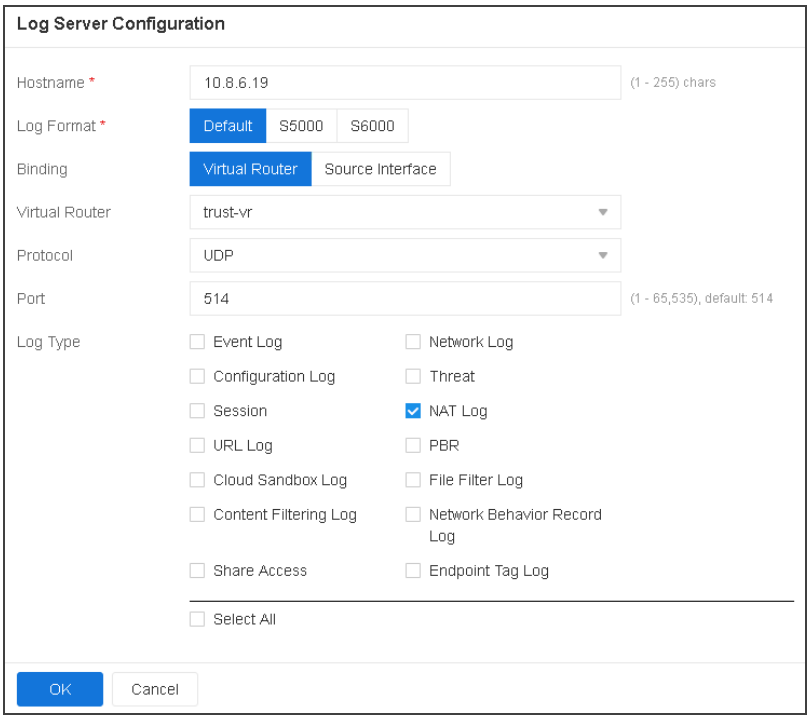
   You can also go to Monitor > Log > Log Management. Click the button behind NAT Log and click  to make corresponding configuration.



To configure the log server, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration** > **Log Server Configuration**.

2. On the **Log Server Configuration** tab, click **New**.

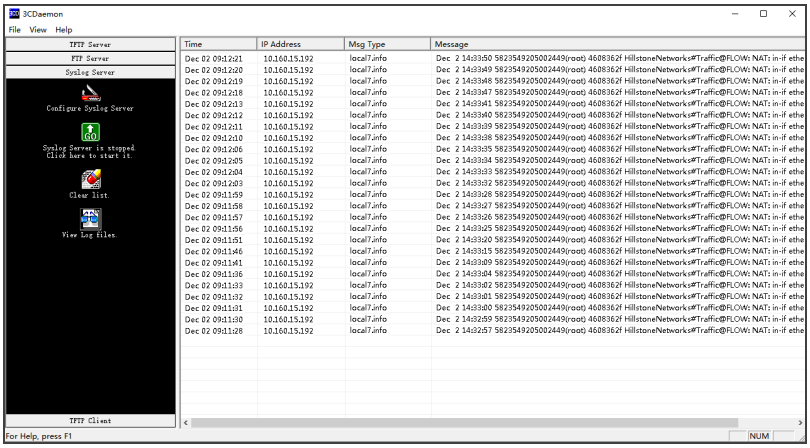


Option	Value
Hostname	Enter the IP address of the PC where the log server is located.
Binding	Virtual Router
Protocol	UDP (the default syslog protocol)
Port	514 (the default syslog port)
Log Type	Select **NAT Log**.

3. Click **OK**.

Step 3: Viewing NAT Logs in the Log Server

- Access the log server. You can see that the log server has received NAT logs.



- Access the directory for saving log files and you can view the saved log files.

Chapter 2 Deploying Your Device

This chapter introduces how a firewall works and its most commonly used scenarios. Understanding the system structure, basic elements and flow chart will help you in better organizing your network and making the most of the firewall product.

- "How a Firewall Works" on Page 100

A firewall has more than one deployment scenario. Each scenario applies to one environment requirement. The usual deployment modes are:

- "Deploying Transparent Mode" on Page 109

  Transparent mode is a situation when the IT administrator does not wish to change his/her existing network settings. In transparent mode, the firewall is invisible to the network. Because no IP address configuration is needed, the firewall only provides security features.

- "Deploying Routing Mode" on Page 119

  Routing mode applies when the firewall offers both routing and NAT functions. In routing mode, the firewall connects two networks typically, an internal network and the Internet, and the firewall interfaces are configured with IP addresses.

- "Deploying Mix Mode" on Page 128

  If a firewall has Layer-2 interfaces and Layer-3 interfaces, it is in mix mode.

- "Deploying Tap Mode" on Page 129

  When an IT administrator only wants the monitor, IPS or statistic function of a firewall, while not a gateway device, using tap mode is the right choice. In tap mode, the firewall is not directly connected within the network.

How a Firewall Works

A firewall is a network security device. It protects a network by controlling the traffic that comes in and out of that network. The basic mechanism of how a firewall works is that allowing or denying the data packet by identifying whether it matches the policy rules or not. Besides security functions, a firewall can also works as a bridging device to connect a trust zone (internal network) and untrust zone (external network).

StoneOS System Architecture

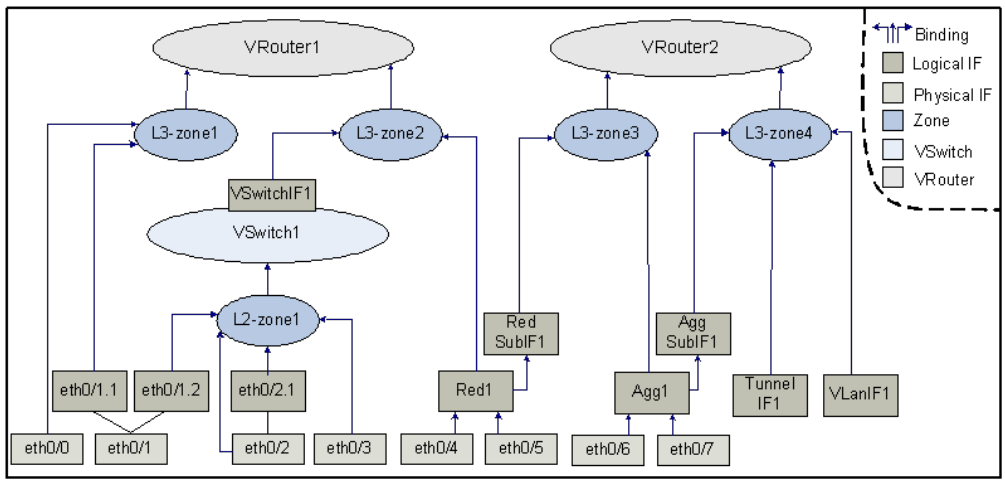
The elements that constitute StoneOS system architecture are:

- **Zone**: Zones divide network into multiple segments, for example, trust (usually refers to the trusted segments such as the Intranet), untrust (usually refers to the untrusted segments where security treats exist).
- **Interface**: Interface is the inlet and outlet for traffic going through security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone. Furthermore, for the Layer 3 security zone, an IP address should be configured for the interface and the corresponding policy rules should also be configured to allow traffic transmission between different security zones. Multiple interfaces can be bound to one security zone, but one interface cannot be bound to multiple security zones.
- **VSwitch**: VSwitch is short for Virtual Switch. A VSwitch functions as a switch in Layer 2. After binding a Layer 2 zone to a VSwitch, all the interfaces in the zone are also bound to the VSwitch. There is a default VSwitch named VSwitch1. By default, all Layer 2 zones will be bound to VSwitch1. You can create new VSwitches and bind Layer 2 zones to VSwitches. Each VSwitch is a Layer 2 forwarding zone with its own MAC address table which supports the Layer 2 traffic transmission for the device. Furthermore, the VSwitchIF helps the traffic to flow between Layer 2 and Layer 3.

- **VRouter**: VRouter is Virtual Router and also abbreviated as VR. A VRouter functions as a router with its own routing table. There is a default VR named trust-vr. By default, all the Layer 3 zones will be bound to trust-vr automatically. The system supports the multi-VR function and the max VR number varies from different platforms. Multiple VRs make the device work as multiple virtual routers, and each virtual router uses and maintains its own routing table.The multi-VR function allows a device to achieve the effects of the address isolating in different route zones and the address overlapping in different VRs, as well as avoiding leakage of route to some extent and enhancing route security of network.

- **Policy**: Policy is used to control the traffic flow in security zones/segments. By default Hillstone devices will deny all traffic in security zones/segments, while the policy can identify which flow in security zones or segments will be permitted, and which will be denied, which is specifically based on policy rules.

For the relationships among interface, security zone, VSwitch and VRouter, see the following diagram:



As shown above, the binding relationships among them are:

- Interfaces are bound to security zones. Interfaces bound to Layer 2 security zones and Layer 3 security zones are known as Layer 2 interfaces and Layer 3 interfaces respectively. One

interface can be only bound to one security zone; interface and its sub interface can belong to different security zones.

- Security zones are bound to a VSwitch or VRouter. Layer 2 security zones are bound to a VSwitch (by default the predefined Layer 2 security zone is bound to the default VSwitch1), and Layer 3 security zones are bound to a VRouter (by default the predefined Layer 3 security zone is bound to the default trust-vr), thus realizing the binding between the interfaces and VSwitch or VR. One security zone can be only bound to one VSwtich or VR.

General Rules of Security Policy

By default, all interfaces, even in the same zone, cannot communicate. Traffic in different zones are not allowed to be transferred either. In order to change the rule, you need to set up new policy rules to allow traffic forwarding.



Notes: To allow bidirectional traffic, you need to set up two policies: one is from source to destination, the other is from destination to source. If there is only one-direction initiative access, the responsive direction only need to respond to that visit, you will need to create only one-way policy (from source to destination).

This part explains what policy is needed to allow interfaces in different zones, VSwitches, or VRouters to communicate. The rules are:

- **Interfaces in the same zone**

  To allow interfaces in the same zone to communicate, you need to create a policy whose source and destination are both the zone which the interfaces belong to.

  For example, to allow eth0/0 and eth0/1 to communicate, you need to create an "allowing" policy with source L3-zone and destination L3-zone.

- **Zones of two interfaces are under the same VSwtich**

  To allow communication of interfaces in different zones under the same VSwitch, you need to create two policies: one policy is to allow traffic from a zone to another; the other policy is

to allow traffic in the opposite direction.

For example, to allow eth0/2 and eth0/3 to communicate, you should create a policy whose source is L2-zone1 and destination is L2-zone2, then create another policy to allow traffic from L2-zone2 to L2-zone1.

- Zones of two interfaces are under different VSwitches

  Each VSwtich has its VSwtich interface (VSwitchIF) which is bound to a Layer-3 zone. To allow interfaces in different zones under different VSwitches to communicate, you need to create an "allowing" policy where the source is the zone of one VSwitchIF and the destination is the zone of the other VSwitchIF. After that, create another policy of the opposite direction.

- Zones of two L3 interfaces are under the same VRouter

  To allow two L3 interfaces to communicate, you need to create a policy allowing one zone to the other zone.

  For example, to allow communication between eth0/0 and eth0/5, you should create a policy from L3-zone1 to L3-zone2, and then create an opposite direction policy.

- Zones of two L3 interfaces are under different VRouters

  To allow two L3 interfaces in two different zones of different VRouters, you need to create a policy with the source being one VRouter and the destination being the other VRouter. Then you create a policy of the opposite direction.

- An L2 interface and an L3 interface under the same VRouter

  To allow communication between an L2 interface and an L3 interface under the same VRouter, you will need to create a policy whose source is the zone which binds the VSwithIF of L2 interface and the destination is the zone of L3 interface. After that, create a policy of the opposite direction.

  For example, to allow eth0/0 and eth0/2 to communicate, create a policy from L3-zone1 to L2-zone1, and its opposite direction policy.

Packet Processing Rule

Forwarding Rule in Layer 2

Forwarding within Layer 2 means it is in one VSwitch. StoneOS system creates a MAC address table for a VSwitch by source address learning. Each VSwitch has its own MAC address table. The packets are forwarded according to the types of the packets, including IP packets, ARP packets, and non-IP-non-ARP packets.

The forwarding rules for IP packets are:

1. Receive a packet.
2. Learn the source address and update the MAC address table.
3. If the destination MAC address is a unicast address, the system will look up the egress interface according to the destination MAC address. And in this case, two situations may occur:
    - If the destination MAC address is the MAC address of the VSwitchIF with an IP configured, system will forward the packet according to the related routes; if the destination MAC address is the MAC address of the VSwitchIF with no IP configured, system will drop the packet.
    - Figure out the egress interface according to the destination MAC address. If the egress interface is the source interface of the packet, system will drop the packet. Otherwise, system will forward the packet from the egress interface.

If no egress interfaces (unknown unicast) is found in the MAC address table, jump to Step 6 directly.

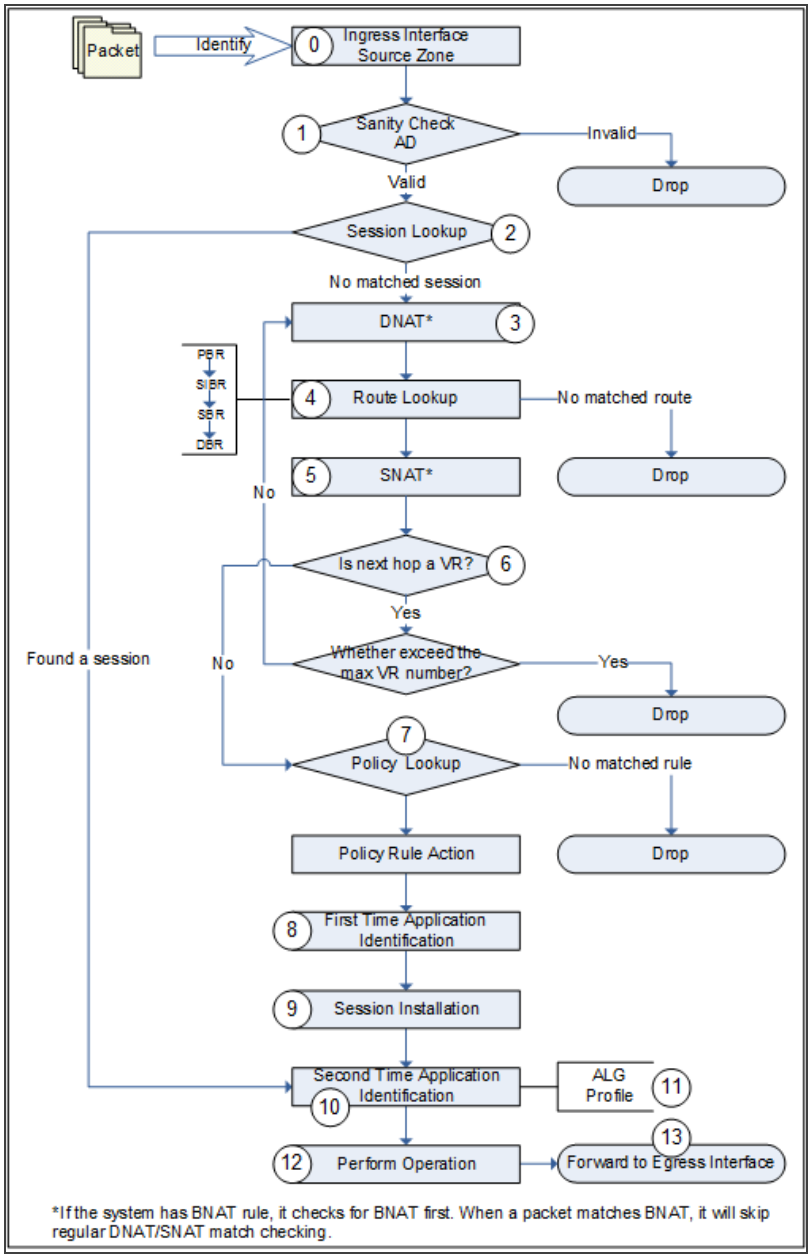
4. Figure out the source zone and destination zone according to the ingress and egress interfaces.

5. Look up the policy rules and forward or drop the packet according to the matched policy rules.

6. If no egress interface (unknown unicast) is found in the MAC address table, system will send the packet to all the other L2 interfaces. The sending procedure is: take each L2 interface as the egress interface and each L2 zone as the destination zone to look up the policy rules, and then forward or drop the packet according to the matched policy rule. In a word, forwarding of unknown unicast is the policy-controlled broadcasting. Process of broadcasting packets and multicasting packets is similar to the unknown unicast packets, and the only difference is the broadcast packets and multicast packets will be copied and handled in Layer 3 at the same time.

For the ARP packets, the broadcast packet and unknown unicast packet are forwarded to all the other interfaces in the VSwitch, and at the same time, system sends a copy of the broadcast packet and unknown unicast packet to the ARP module to handle.

Forwarding Rule in Layer 3



0. Identify the logical ingress interface of the packet to determine the source zone of the packet. The logical ingress interface may be a common interface or a sub-interface.

1. System performs sanity check to the packet. If the attack defense function is enabled on the source zone, system will perform AD check simultaneously.

2. Session lookup. If the packet belongs to an existing session, system will perform Step 11 directly.

3. DNAT operation. If a DNAT rule is matched, system will mark the packet. The DNAT translated address is needed in the step of route lookup.
   *Note: If the system has static 1-to-1 BNAT rule, BNAT rule is checked before other NAT rules. If a packet matches BNAT, it will be processed in accordance with this rule's configuration. It will skip the regular DNAT rule checking.

4. Route lookup. The route lookup order from high to low is: PBR > SIBR > SBR > DBR > ISP route.
   Until now, the system has known the logical egress and destination zone of the packet.

5. SNAT operation. If a SNAT rule is matched, system will mark the packet.
   *Note: If the system has static 1-to-1 BNAT rule, BNAT rule is checked before other NAT rules. If a packet matches BNAT, it will be processed in accordance with this rule's configuration. It will skip the regular SNAT rule checking.

6. VR next hop check. If the next hop is a VR, system will check whether it is beyond the maximum VR number (current version allows the packet traverse up to three VRs). If it is beyond the maximum number, system will drop the packet; if it is within the maximum number range, return to Step 4. If the next hop is not a VR, go on with policy lookup.

7. Policy lookup. System looks up the policy rules according to the packet’s source/destination zones, source/destination IP and port, and protocol. If no policy rule is matched, system will drop the packet; if any policy rule is matched, the system will deal with the packet as the rule specified. And the actions can be one of the followings:

- Permit: Forward the packet.
- Deny: Drop the packet.
- Tunnel: Forward the packet to the specified tunnel.
- Fromtunnel: Check whether the packet originates from the specified tunnel. System will forward the packet from the specified tunnel and drop other packets.
- WebAuth: Perform WebAuth on the specified user.

8. First time application identification. System tries to identify the type of the application according to the port number and service specified in the policy rule.
9. Establish the session.
10. If necessary, system will perform the second time application identification. It is a precise identification based on the packet contents and traffic action.
11. Application behavior control. After knowing the type of the application, system will deal with the packet according to the configured profiles and ALG.
12. Perform operations according to the records in the session, for example, the NAT mark.
13. Forward the packet to the egress interface.

Deploying Transparent Mode

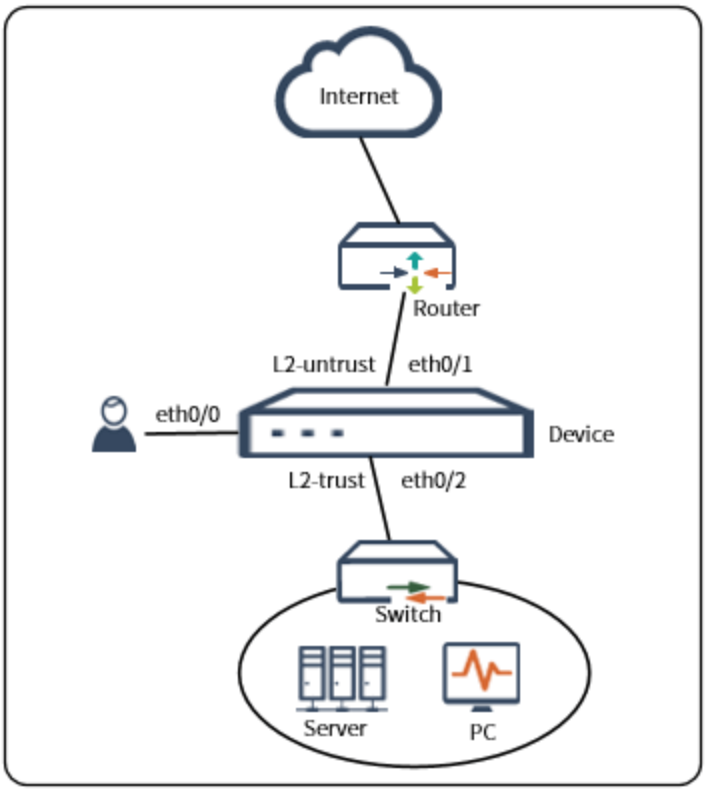
Transparent mode is also known as bridge mode or transparent bridging mode. Transparent mode is used when the IT administrator does not wish to change the existing network layout. Normally, the existing network has already set up routers and switches. The firewall will be used as a security device.

Transparent mode has the following advantages:

- No need to change IP addresses
- No need to set up NAT rule

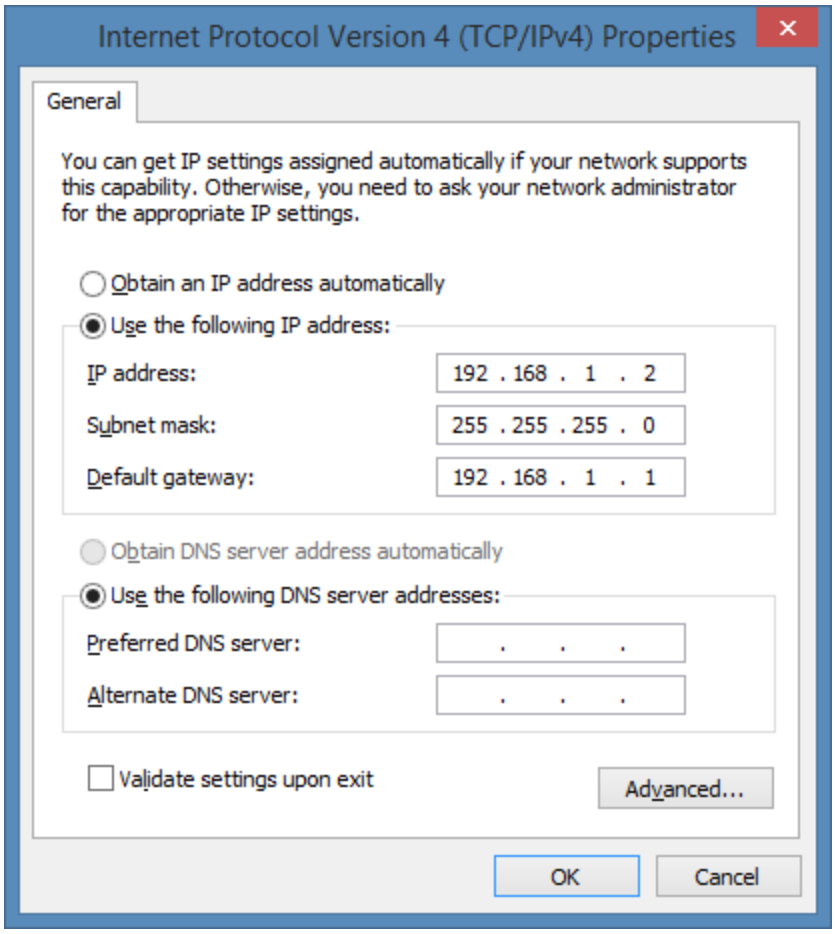
Under normal circumstances, the firewall in transparent mode is deployed between the router and the switch of the protected network, or it is installed between the Internet and a company's router. The internal network uses its old router to access the Internet, and the firewall only provides security control features.

This section introduces a configuration example of a firewall deployed between a router and a switch. In this example,the administrator uses eth0/0 to manage firewall. The firewall's eth0/1 is connected to router (which is connecting to the Internet) and eth0/2 is connected to a switch (which is connecting to internal network).



Step 1: Initial log in the firewall

1. In the administrator's Ethernet properties, set the IPv4 protocol as below.



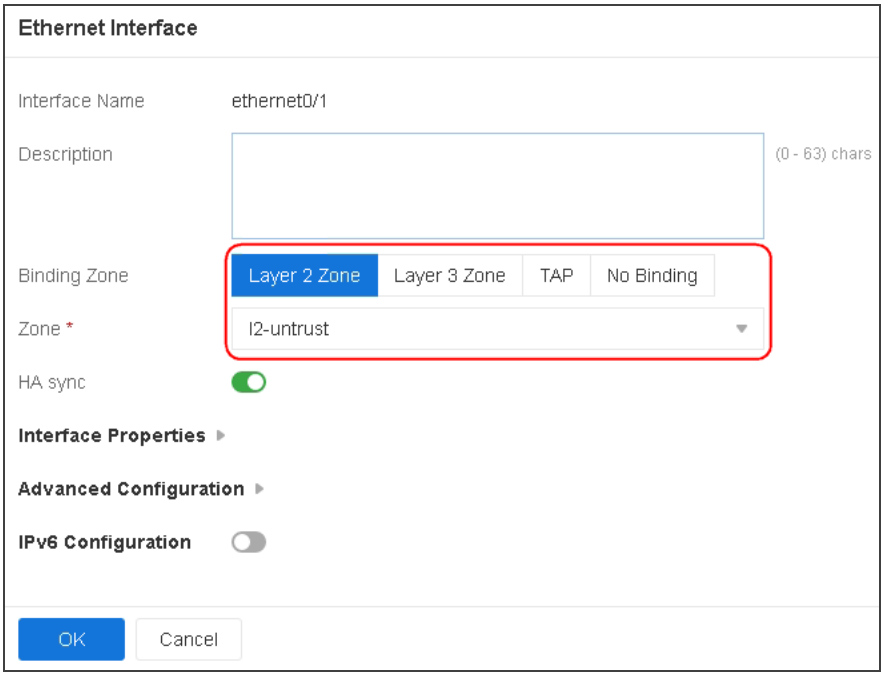
2. Connect an RJ-45 Ethernet cable from the computer to the eth0/0 of the device.
3. In the browser's address bar, type "https://192.168.1.1" and press **Enter**.
4. In the login interface, type the default username and password: hillstone/hillstone.
5. Click **Login**, follow the prompts to change the default password, and then log in again with the new password.

Step 2: Configure interface and zone

- Configure eth0/1 as an Internet connected interface.

    1. Select **Network > Interface**.

    2. Double click ethernet0/1, and configure in the prompt.

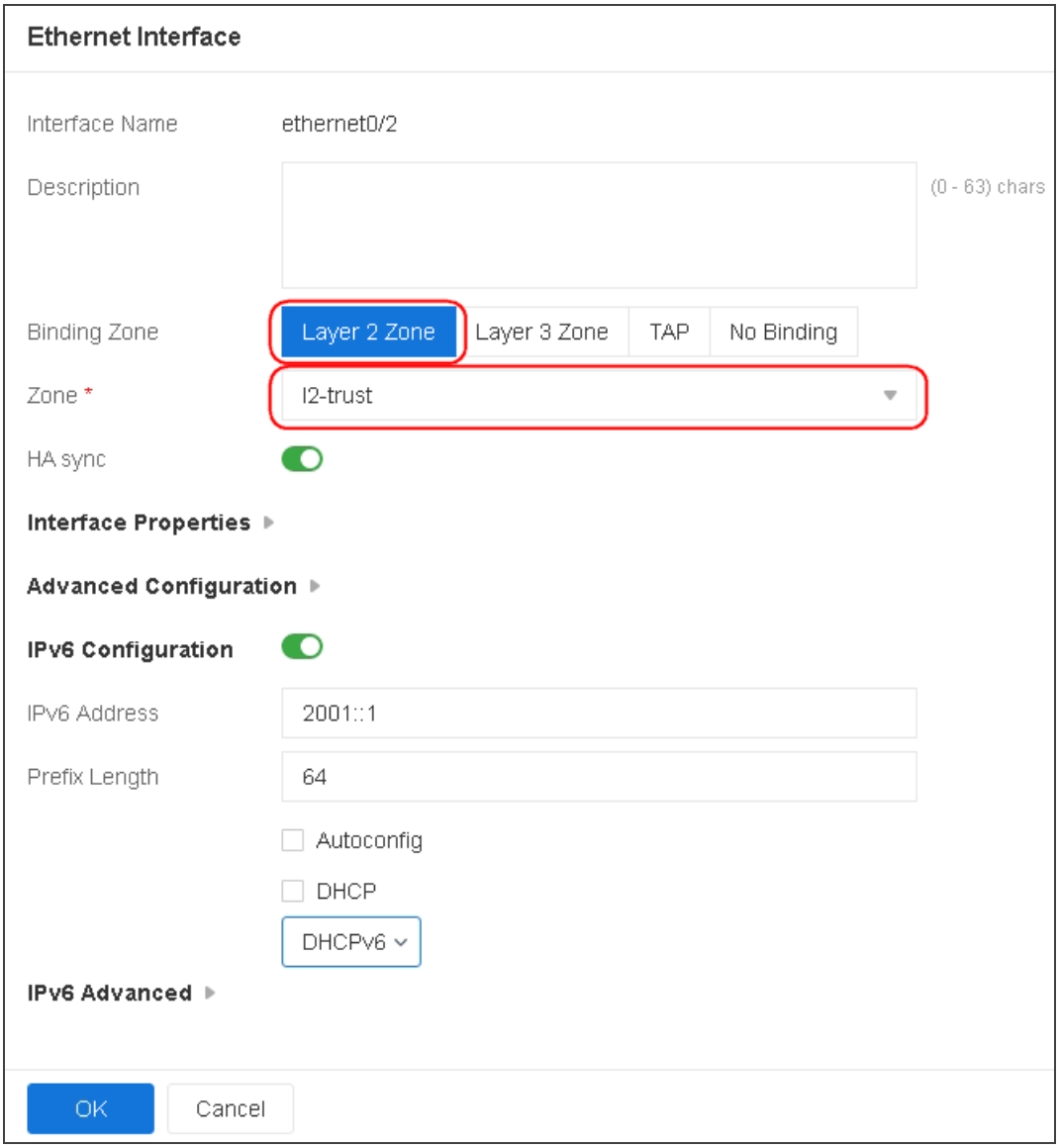


    3. Click **OK**.

- Configure eth0/2 as a private network connected interface.

    1. Select **Network > Interface**.

    2. Double click ethernet0/2, and configure in the prompt.



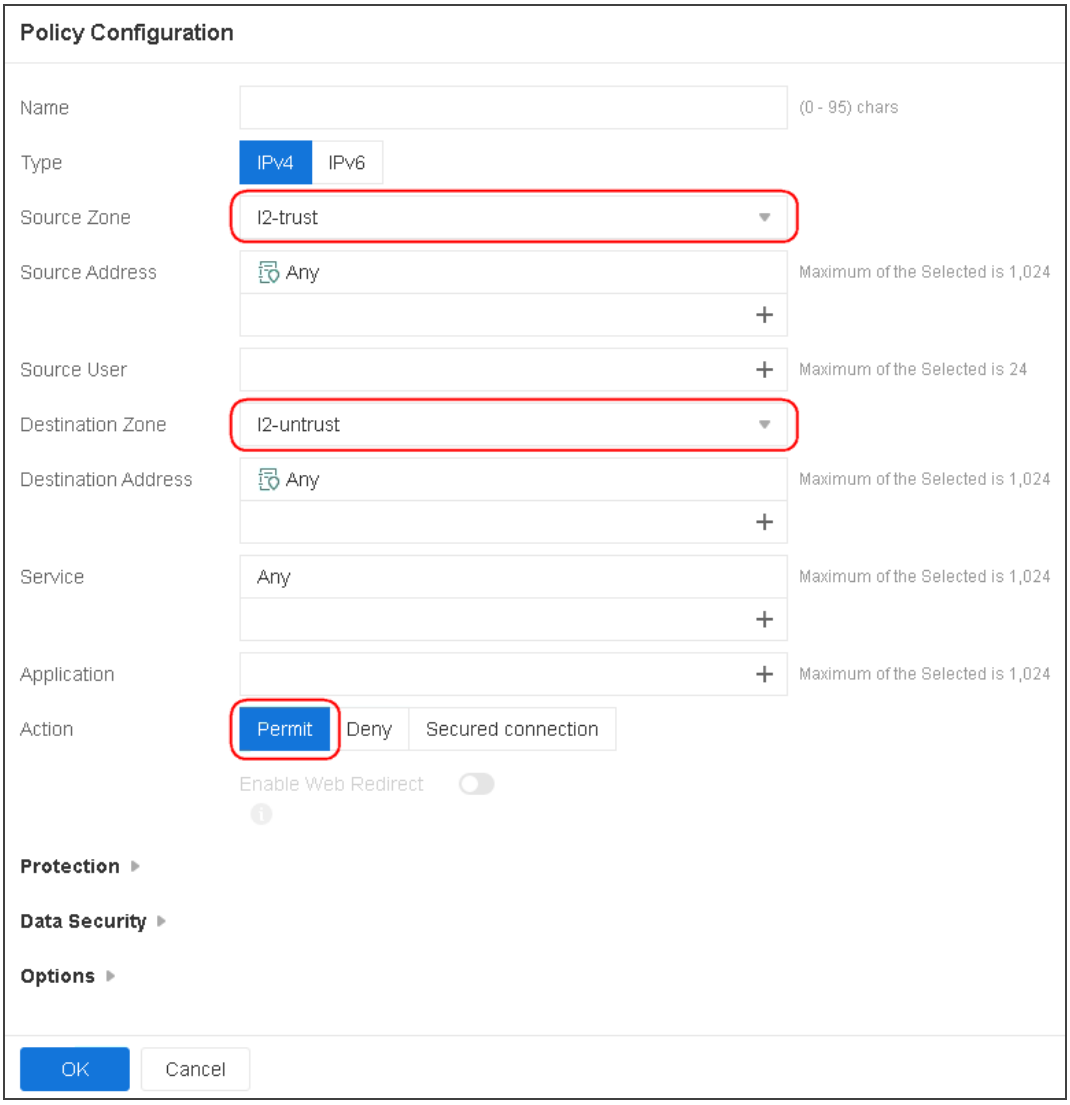
    3. Click **OK**.

Step 3: Configuring policies

- Create a policy to allow visiting the Internet.

    1. Select **Policy > Security Policy>Policy**.

    2. Click **New**,select Policy from the drop-down list.

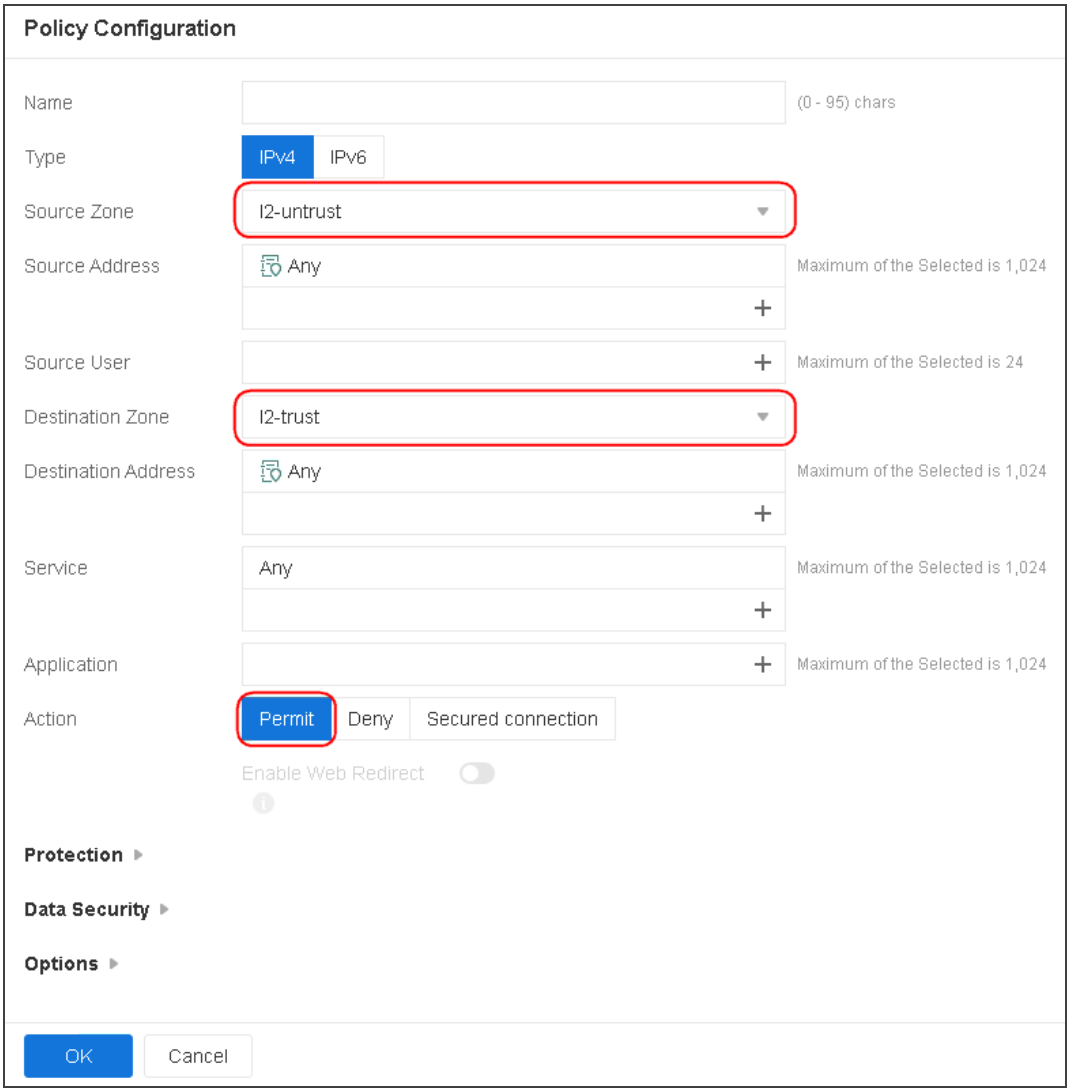


    3. Click **OK**.

- Create a policy to allow the Internet to visit a private network.

    1. Select **Policy > Security Policy**.

    2. Click **New**.



    3. Click **OK**.

- The two policies above ensure communication between a private network and the Internet. If you want to set up more details, e.g. to limit P2P download, you can add more policies and

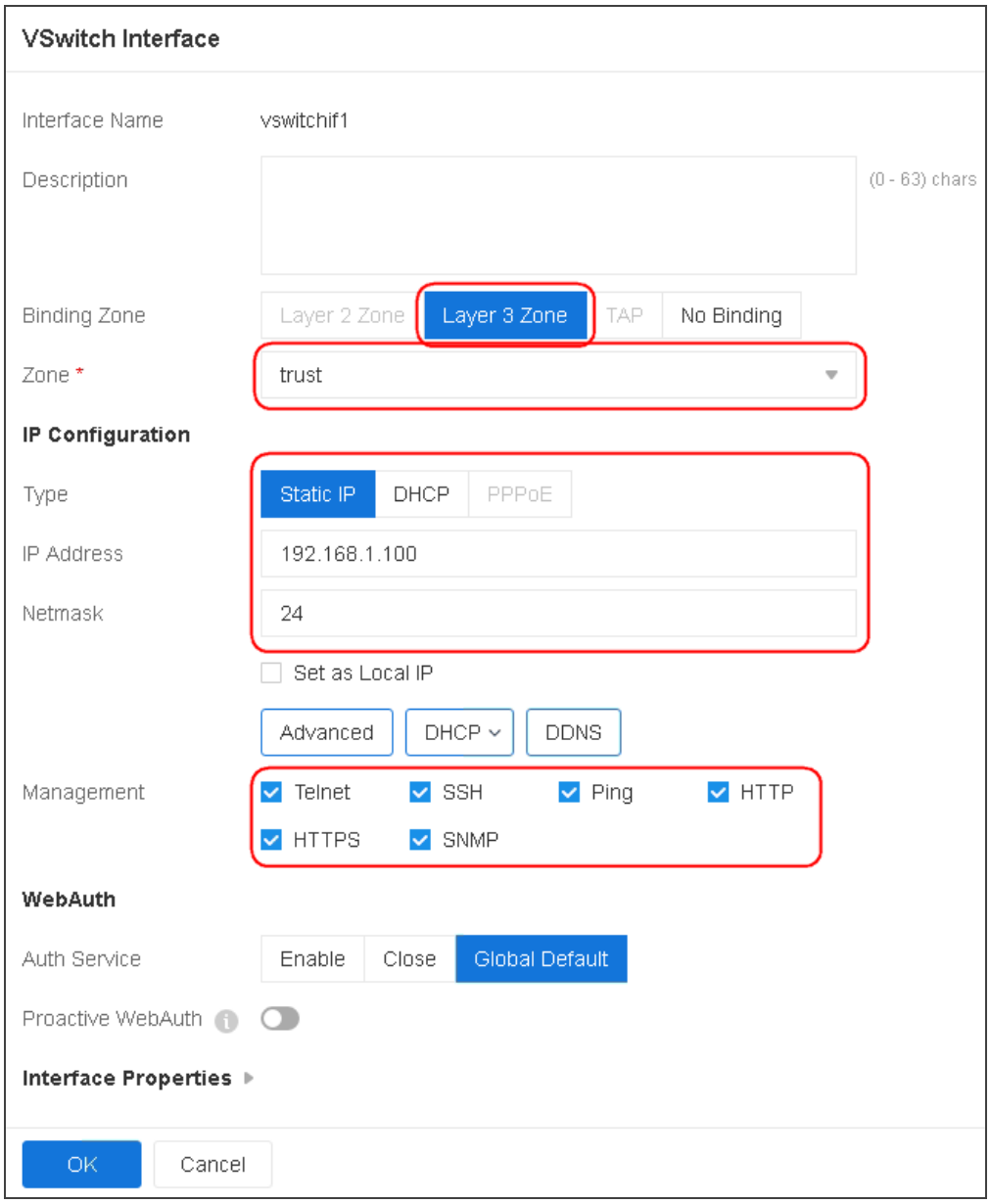
overlap the new policies with the old ones. The match sequence of policies is determined by their position in the policy list, not their ID numbers.

(Optional) Step 4: Configuring VSwitch Interface for managing the firewall.

If you want any PC in the private network to visit and configure the firewall, you can configure a VSwitch interface as a management interface.

1. Select **Network > Interface**.

2. Double click vswtichif1.



Notes: When configuring **IP Configuration**, set an IP address in the same subnet of the private network.

3. Click **OK**.

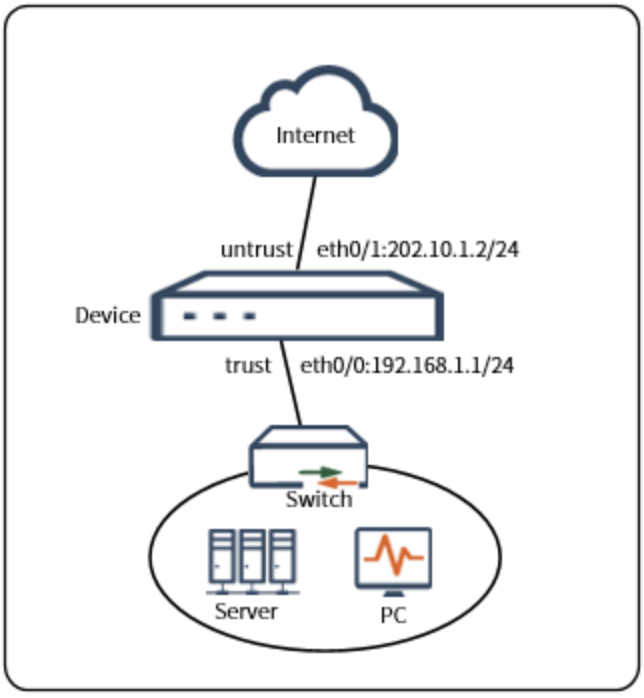
4. With any PC in the private network, enter the IP address of vswitchif1, and you will visit the firewall web user interface.

Deploying Routing Mode

Routing mode deployment often uses the NAT function, so it is also called NAT mode. In routing mode, each interface has its IP address which means interfaces are in the layer 3 zone. A firewall in routing mode can work as a router and a security devcie.

Routing mode is mostly used when the firewall is installed between an internal network and the Internet.

The example which is based on the below topology shows you how to connect and configure a new Hillstone device in routing mode. The device connects a private network to the Internet.



Step 1: Connecting to the device

1. Connect one port (e.g. eth0/1) of the Hillstone device to your ISP network. In this way, "eth0/1" is in the untrust zone.
2. Connect your internal network to another Ethernet interface (e.g. eth0/0) of the device. This means "eth0/0" is connected to the trust zone.

3. Power on the Hillstone device and your PCs.

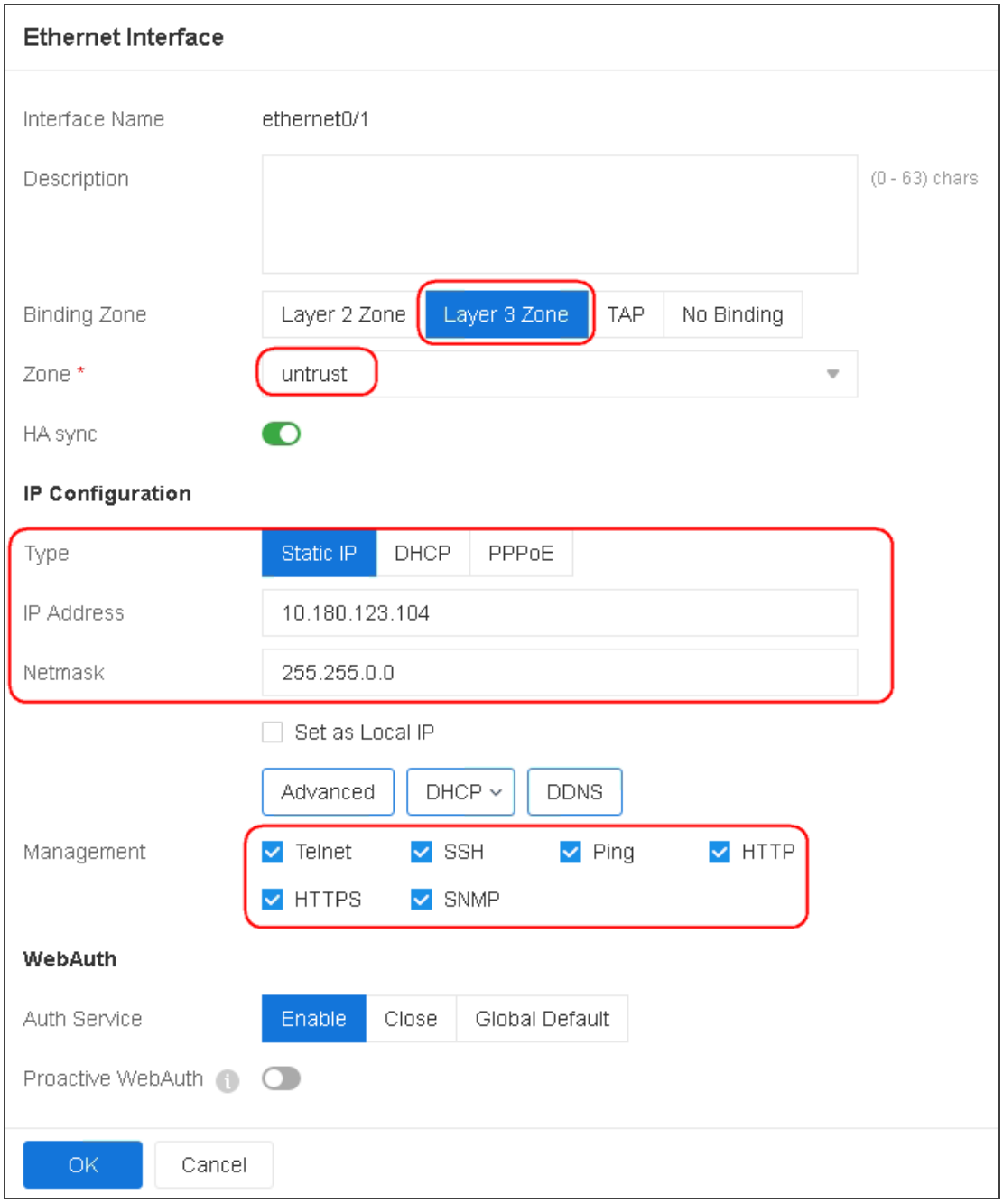
4. If one of the internal interfaces already has been configured with an IP address, use a browser to visit that address from one of your internal PCs.
   If it is a new device, use the methods in "Log in to WebUI" on Page 12 to visit.

5. Enter "hillstone" for both the username and the password.

Step 2: Configuring interfaces

1. Go to **Network > Interface**.

2. Double click **ethernet0/1**.



Option	Value
Binding Zone	L3-zone

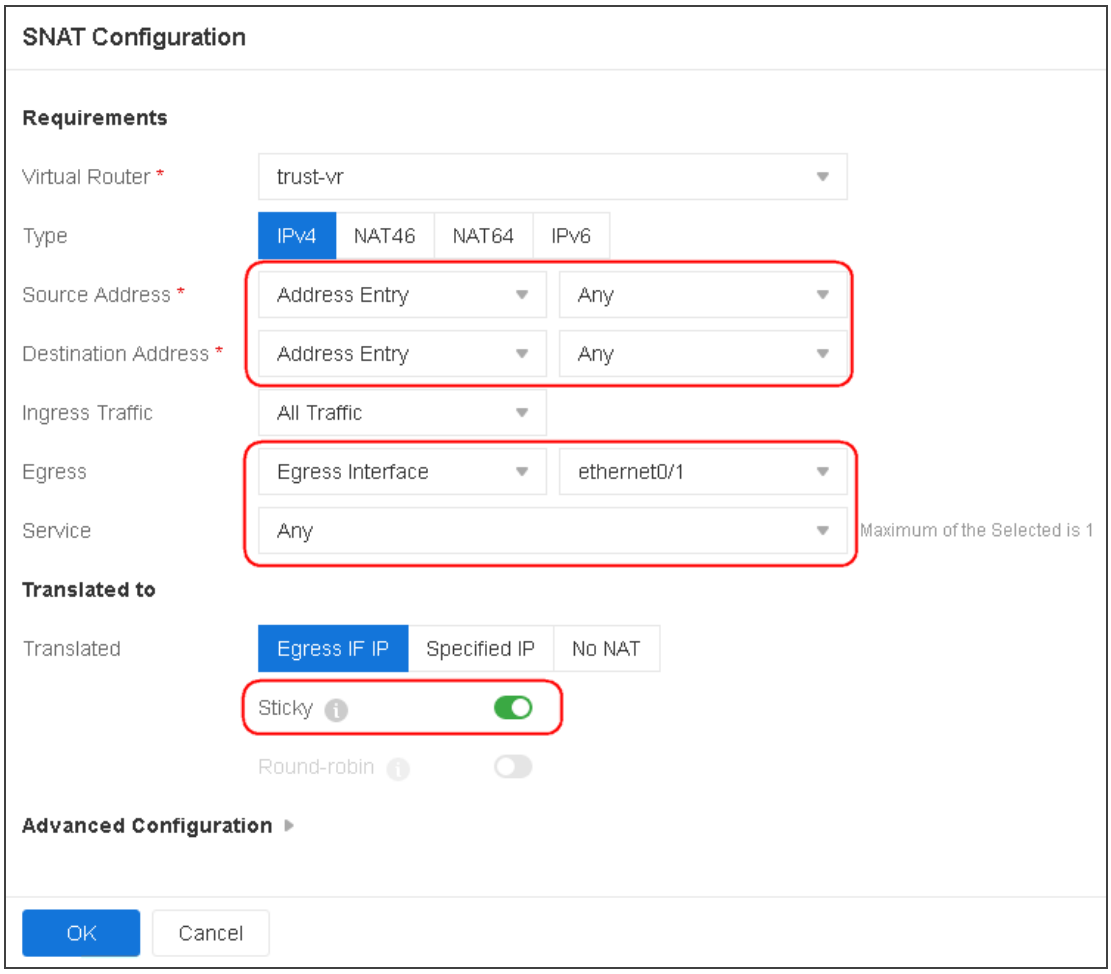
Option	Value
Zone	untrust
Type	Static IP
IP Address	202.10.1.1 (public IP address provided by your ISP)
Netmask	255.255.255.0
Management	Select the protocols that you want to use to access the device.

3. Click **OK**.

Step 3: Creating a NAT rule to translate internal IP to public IP

1. Go to **Policy > NAT > SNAT**.

2. Select **New**



Option	Value
Source Address	Address Entry, Any
Destination Address	Address Entry, Any
Egress	Egress interface, ethernet 0/1

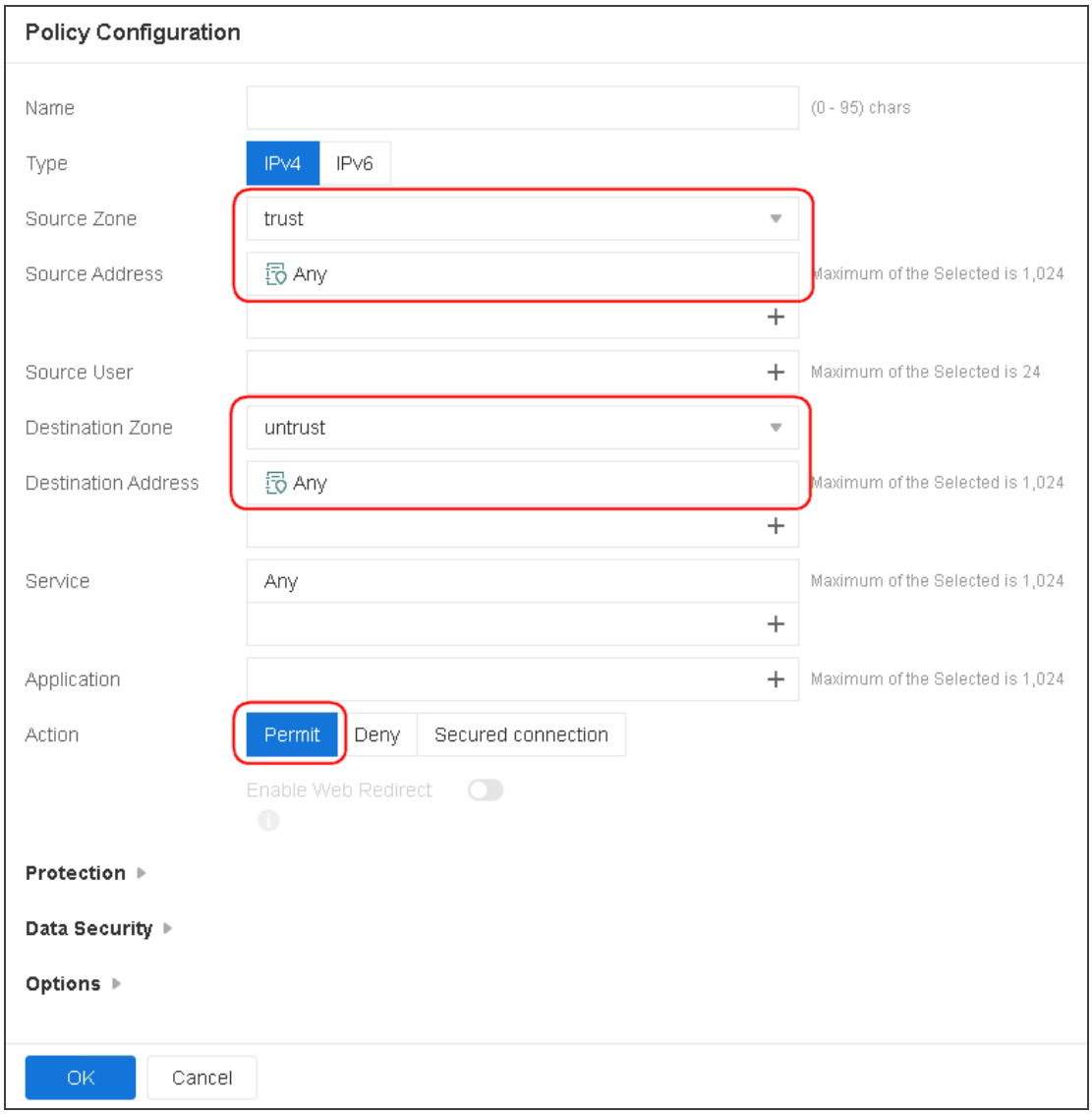
Option	Value
Translated	Egress IP
Sticky	Enable

3. Click **OK**.

Step 4: Creating a security policy to allow internal users to access the Internet.

1. Go to **Policy > Security Policy>Policy**.

2. Click **New**,select **Policy** from the drop-down list.



Source Information	
Zone	trust
Address	Any
Destination Information	
Zone	untrust

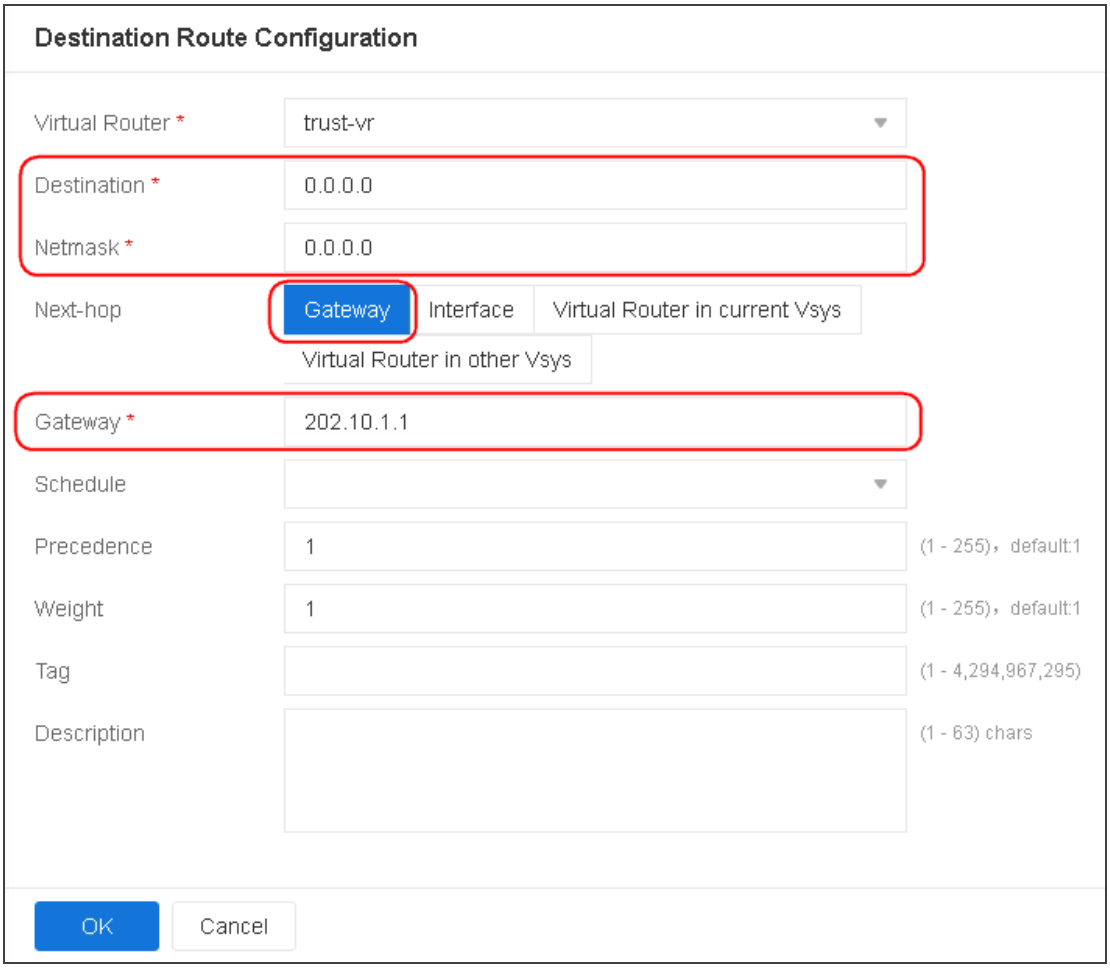
Address	Any
Other Information	
Service/Service Group	Any
APP/APP Group	-----
Action	Permit

3. Click OK.

Step 5: Configuring a default route

1. Go to **Network >Routing > Destination Route**.

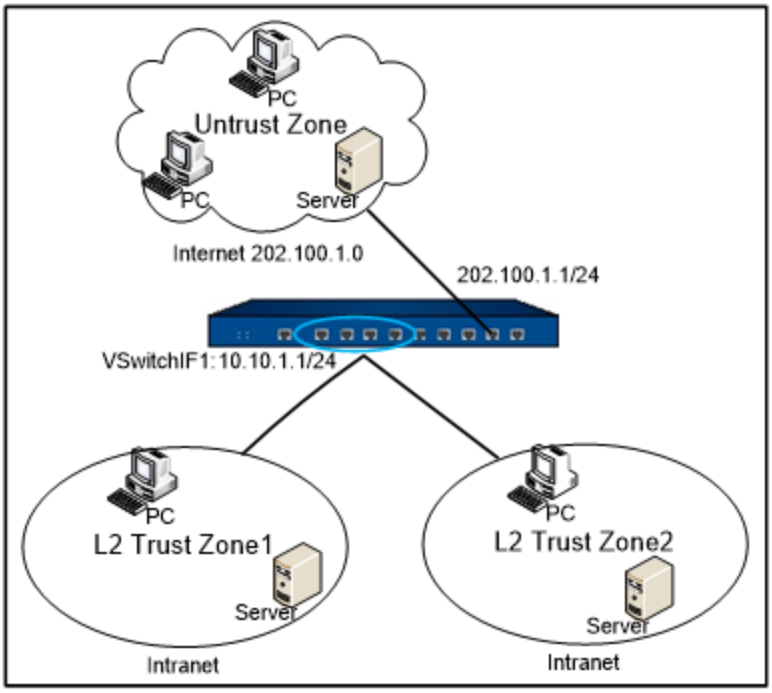
2. Click **New**.



Option	Value
Destination	0.0.0.0 (means all network)
Subnet Mask	0.0.0.0 (means all subnets)
Gateway	202.10.1.1 (gateway provided by your ISP)

Deploying Mix Mode

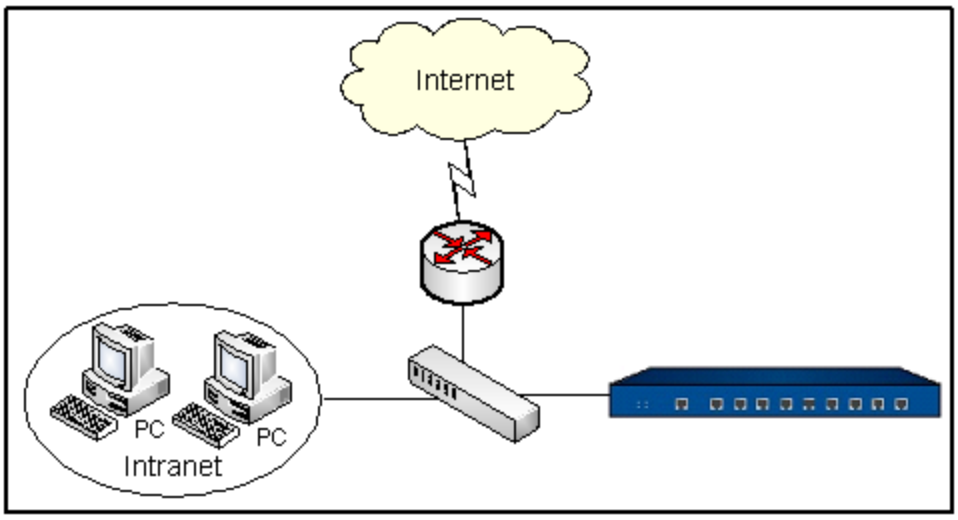
If the firewall has both L2 interfaces (transparent mode) and L3 interfaces (routing mode), the firewall is in mix mode.



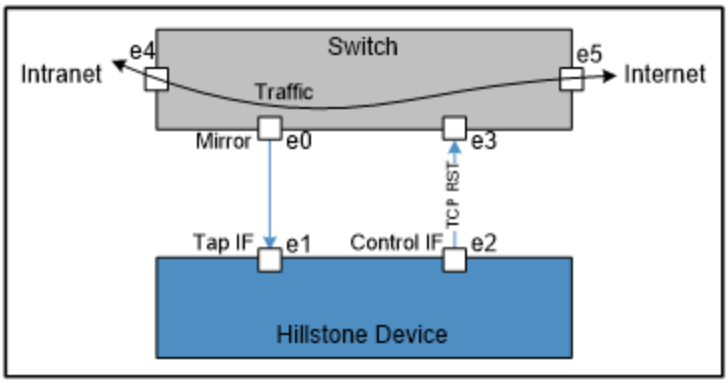
To configure a mix mode, you need to combine the routing mode of the deployment methods with the transparent mode. Please refer to these two modes.

Deploying Tap Mode

In most cases, the security device is deployed within the network as a serial node. However, in some other scenarios, an IT administrator would just want the auditing and statistical functions like IPS, antivirus, and Internet behavior control. For these features, you just need to connect the device to a mirrored interface of a core network. The traffic is mirrored to the security device for auditing and monitoring.



The bypass mode is created by binding a physical interface to a tap zone. Then, the interface becomes a bypass interface.



Use an Ethernet cable to connect e0 of the Switch with e1 of the Hillstone device. The interface e1 is the bypass interface and e2 is the bypass control interface. The interface e0 is the mirror interface of the switch.The switch mirrors the traffic to e1 and the Hillstone device will monitor,

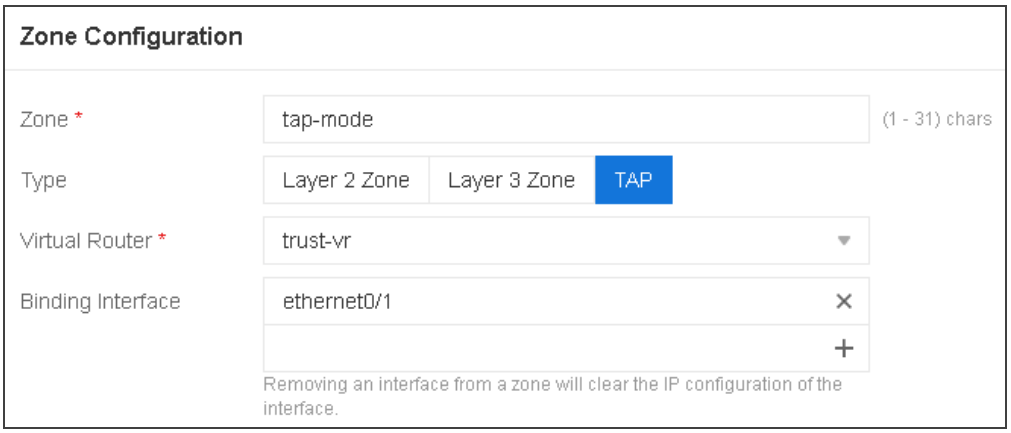
scan, and log the traffic received from e1. After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, viruses, or illegal network behaviors, it will send a TCP RST packet from e2 to the switch to tell it to reset the connections.

Notes: Before configuring tap mode in the device, you need to set up an interface mirroring your primary switch. Mirror the traffic of the switch from e0 to e1, and the device can scan, monitor and count the mirrored traffic.

Here provides an example of monitoring IPS in tap mode.

Step 1: Creating tap mode by binding an interface

1. Select **Network > Zone**, and click **New**.



Option	Value
Zone	enter a name, e.g. "tap-zone" .
Type	TAP
Binding Interface	Select the bypass interface (only a physical interface, aggregate interface or redundant interface can apply, sub-interface is not allowed).

2. Click **OK**.

Step 2: Creating an IPS rule

1. Select **Object > Intrusion Prevention System**.
2. Click **New**.
3. Enter the rule name.
4. Configure the signatures settings.
5. Configure the protocol settings.
6. Click **OK** to complete IPS rule configuration.

Step 3: Add IPS rule into Tap zone

1. Select **Network > Zone**, and double-click the tap zone created in step 1.
2. In the Treat Prevention tab, enable IPS and select the IPS rule created.



3. Click **OK**.

(Optional) Block traffic in switch

A bypass control interface is used to send control packets (TCP RST packet is supported in current version). After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, viruses, or illegal network behaviors, it will send a TCP RST packet from e2 to the switch to tell it to reset the connections.

By default, the bypass interface itself is the control interface. However, you may also change the control interface.

To change a bypass control interface, you can only use the command line interface:

tap control-interface *interface-name*

- *interface-name* - Specifies which interface is used as the bypass control interface.

Chapter 3 Dashboard

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

The dashboard shows the system and threat information. The layout of the dashboard is shown below:

Customization

You can customize the dashboard display function or modify the function area location as needed.

- To customize the dashboard display function:

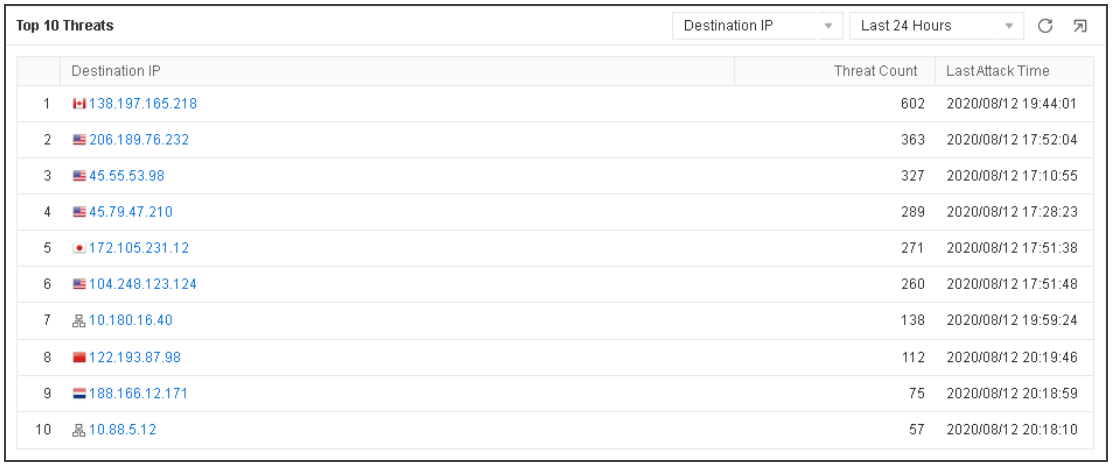
    1. Click **Customize** at the top-right corner.
    2. Select the function check box from the expanded list.

- To modify the function area location:

    1. Hover your mouse over the title part in the ribbon.
    2. When  appears, press and hold the mouse functional area , the regional location to be displayed .

Threats

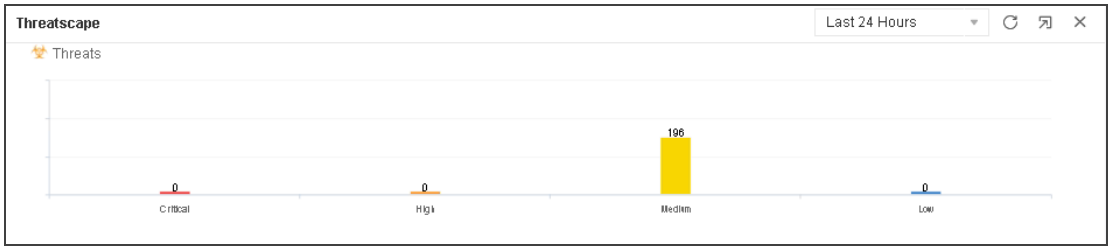
Display the top 10 threats information within the specified period.



- Click Destination IP to specify the type of display: Destination IP, Source IP or Threat Name.

Threatscape

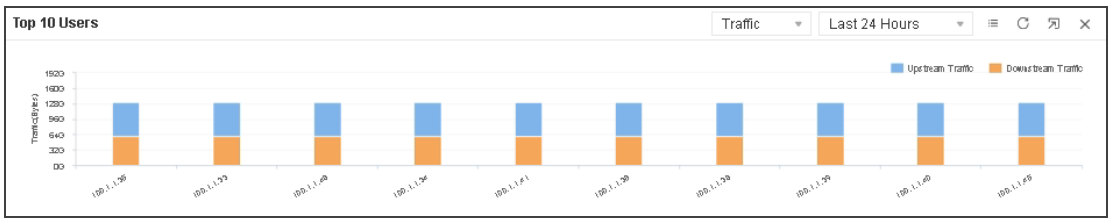
The threat information statistic chart is displayed within the specified period.



- Click the column to jump to the iCenter page, and the list will display the corresponding threat level.

User

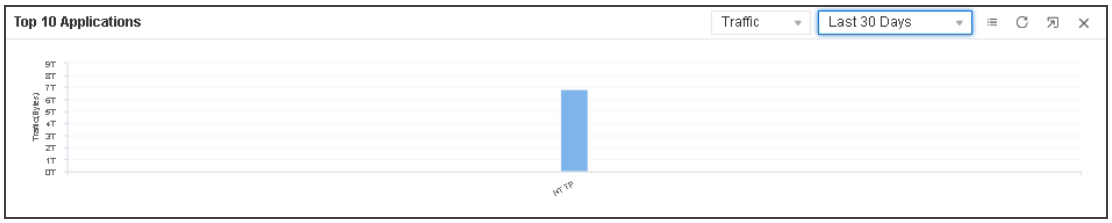
Display the top 10 user traffic information within the specified period.



- Specify the type of display: by Traffic or by Concurrent Sessions from the drop-down menu.
- Click and , switch between the table and the bar chart.
- Hover your mouse over a bar, to view users' upstream traffic, downstream traffic, total traffic or concurrent sessions.

Application

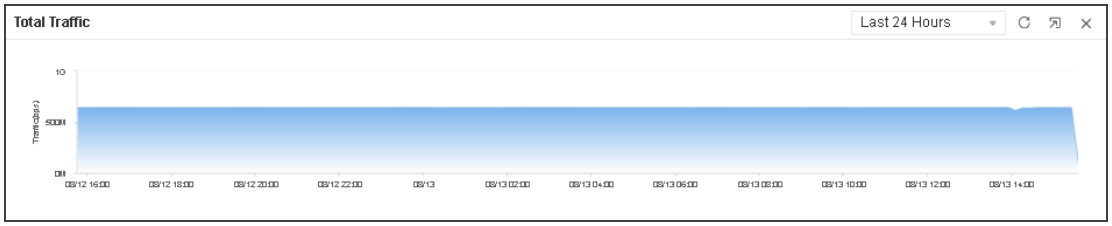
Display the top 10 application traffic information within the specified period.



- Specify the type of display: by Traffic or by from the drop-down menu.
- Click and , switch between the table and the bar chart.
- Hover your mouse over a bar, to view users' total traffic .

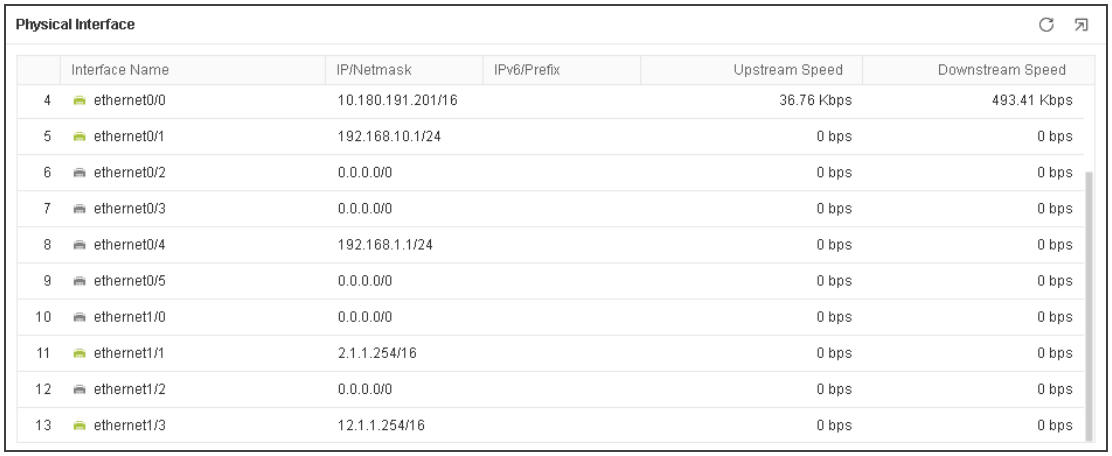
Total Traffic

Show the Total Traffic within the specified period .



Physical Interface

Display the statistical information of interfaces, including the interface name, IP address, upstream speed, downstream speed, and total speed.



	Interface Name	IP/Netmask	IPv6/Prefix	Upstream Speed	Downstream Speed
4	ethernet0/0	10.180.191.201/16		36.76 Kbps	493.41 Kbps
5	ethernet0/1	192.168.10.1/24		0 bps	0 bps
6	ethernet0/2	0.0.0.0/0		0 bps	0 bps
7	ethernet0/3	0.0.0.0/0		0 bps	0 bps
8	ethernet0/4	192.168.1.1/24		0 bps	0 bps
9	ethernet0/5	0.0.0.0/0		0 bps	0 bps
10	ethernet1/0	0.0.0.0/0		0 bps	0 bps
11	ethernet1/1	2.1.1.254/16		0 bps	0 bps
12	ethernet1/2	0.0.0.0/0		0 bps	0 bps
13	ethernet1/3	12.1.1.254/16		0 bps	0 bps

System and Signature Database

System Information

System information include.

- Serial number: The serial number of the device.
- Host name: The host name of the device.
- Product Category: The category name of the product. Click button, in the < Configure> Page, enter a user-defined product name with a range of 0-128 characters in the product category text box. Click **OK** button. After modification, the login page will display the customized product name.
- Platform: The platform type of the device.
- System Time: The time of system.
- System Uptime: The running time of system.
- HA State: The HA State of device:

- Standalone: Non-HA mode which represents HA is disabled.
- Init: Initial state.
- Hello: Negotiation state which represents the device is negotiating the relationship between master and backup.
- Master: Master state which represents current device is master.
- Backup: Backup state which represents current device is backup.
- Failed: Fault state which represents the device is failed.
- Disabled： Disabled state which represents the interface is disabled. Only Peer Active-Active mode has this state.

- Firmware: The version number and version time of the firmware running on the device.
- Boot File: The version name of the current device boot file and the time when the file was compiled.

Signature DB Information

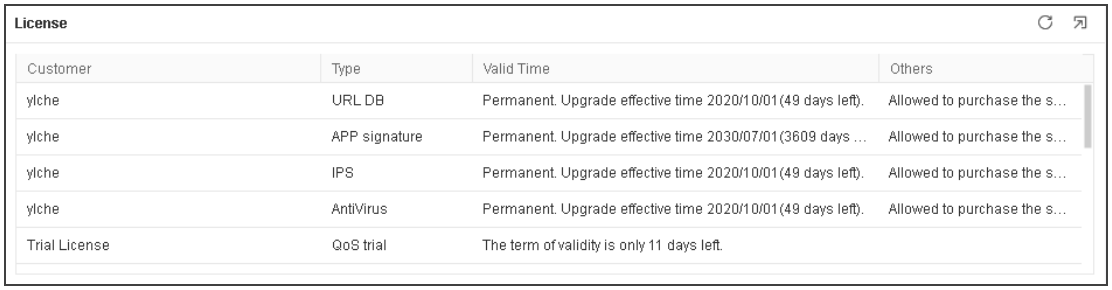
Signature database information include.

- Check Immediately: Click the **Check Immediately** to update and display the latest version number of the signature library.
  Note: The signature database license should been activated and the system already has a signature library version.
- Anti Virus Signature: The version number and time of the anti virus signature database.
- IPS Signature: The version number and time of the IPS signature database.
- Botnet Prevention Signature Database: The version number and time of the botnet prevention signature database.

- URL Category Database: The version number and time of the URL category database.
- Application Signature: The version number and time of the application signature database.
- Sandbox Whitelist Database: The version number and time of the sandbox whitelist database.
- IP Reputation Database: The version number and time of the IP reputation database.

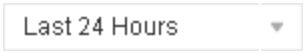
License

Display the detailed information of installed licenses.



- Customer: Displays the name of the customer who applied for the license.
- Type: Displays the type of license.
- Valid Time: Displays the valid time of license.
- Others: Displays additional notes for the license.

Specified Period

System supports the predefined time cycle and the custom time cycle. Click 

on the top right corner of each tab to set the time cycle.

- Realtime: Display the real-time statistical information.
- Last Hour: Display the statistical information within the latest 1 hour.

- Last Day: Display the statistical information within the latest 1 day.
- Last Month: Display the statistical information within the latest 1 month.

In the top-right corner, you can set the refresh interface of the displayed data.

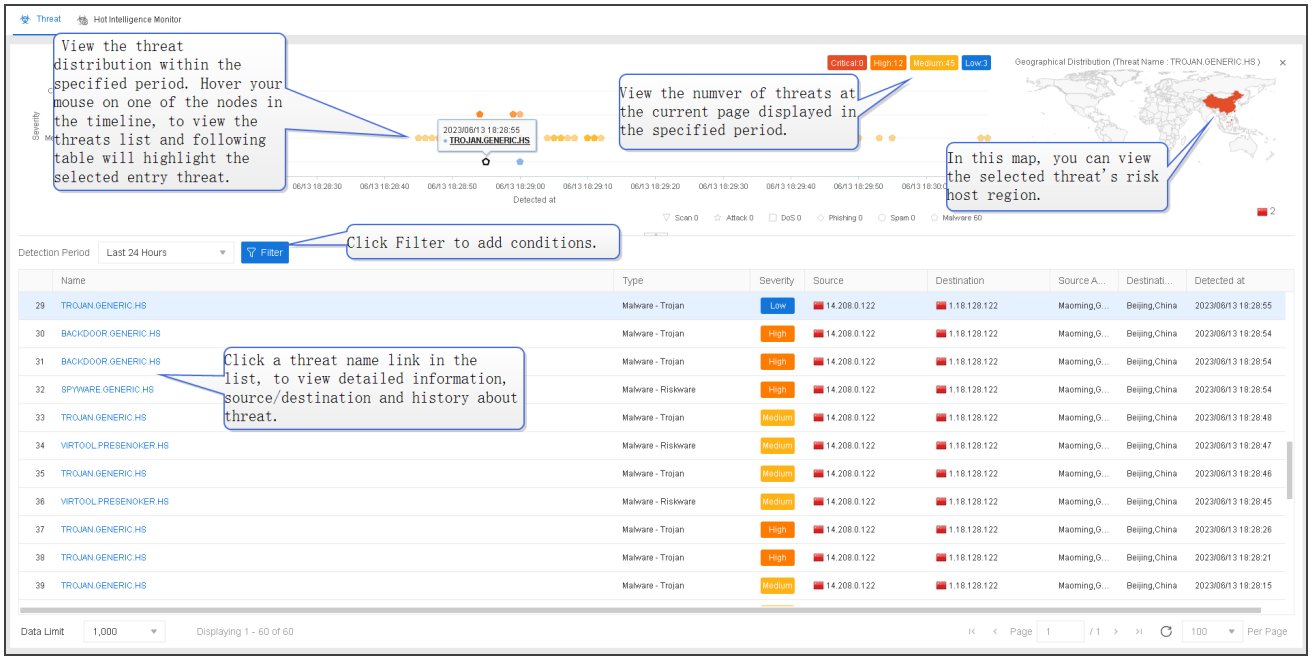
Chapter 4 iCenter

This feature may not be available on all platforms. Please check actual page in system to see whether your device delivers this feature.

The multi-dimensional features show threats to the whole network in depth. threats of the whole network.

Threat

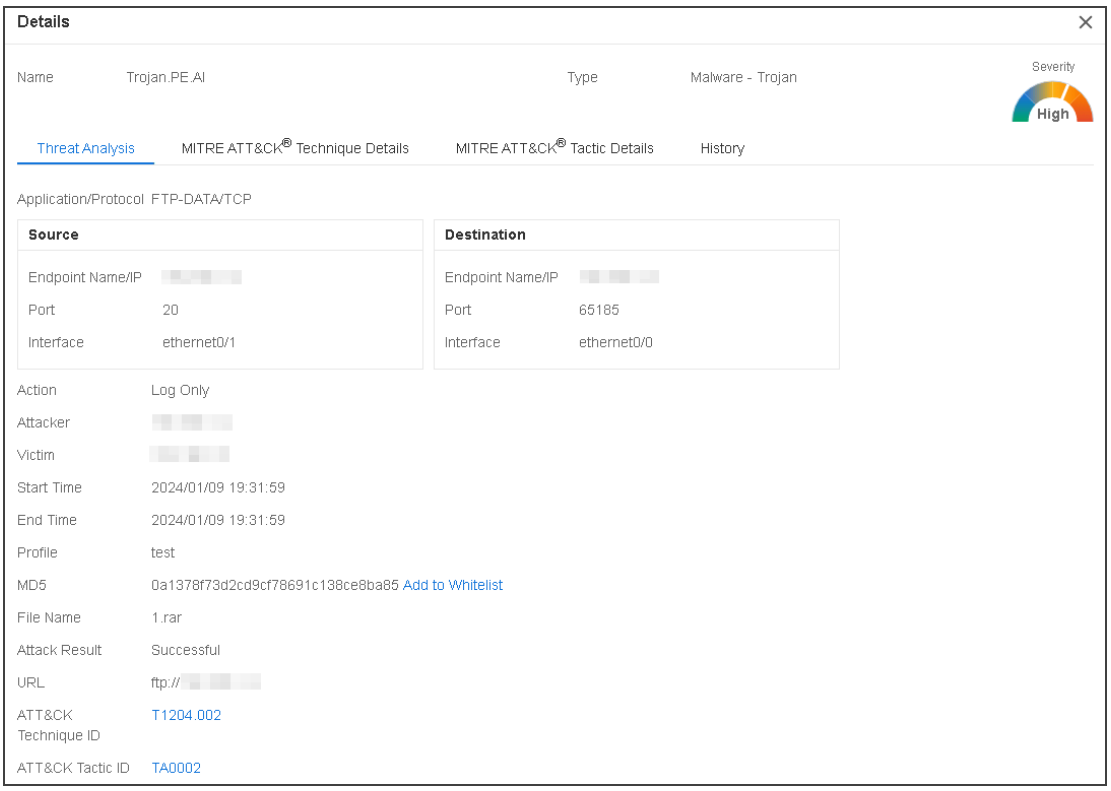
Threats tab statistics and displays the all threats information of the whole network within the "Specified Period" on Page 137. Click **iCenter**.



Click a threat name link in the list to view the detailed information , source/destination, knowledge base and history about the threat.

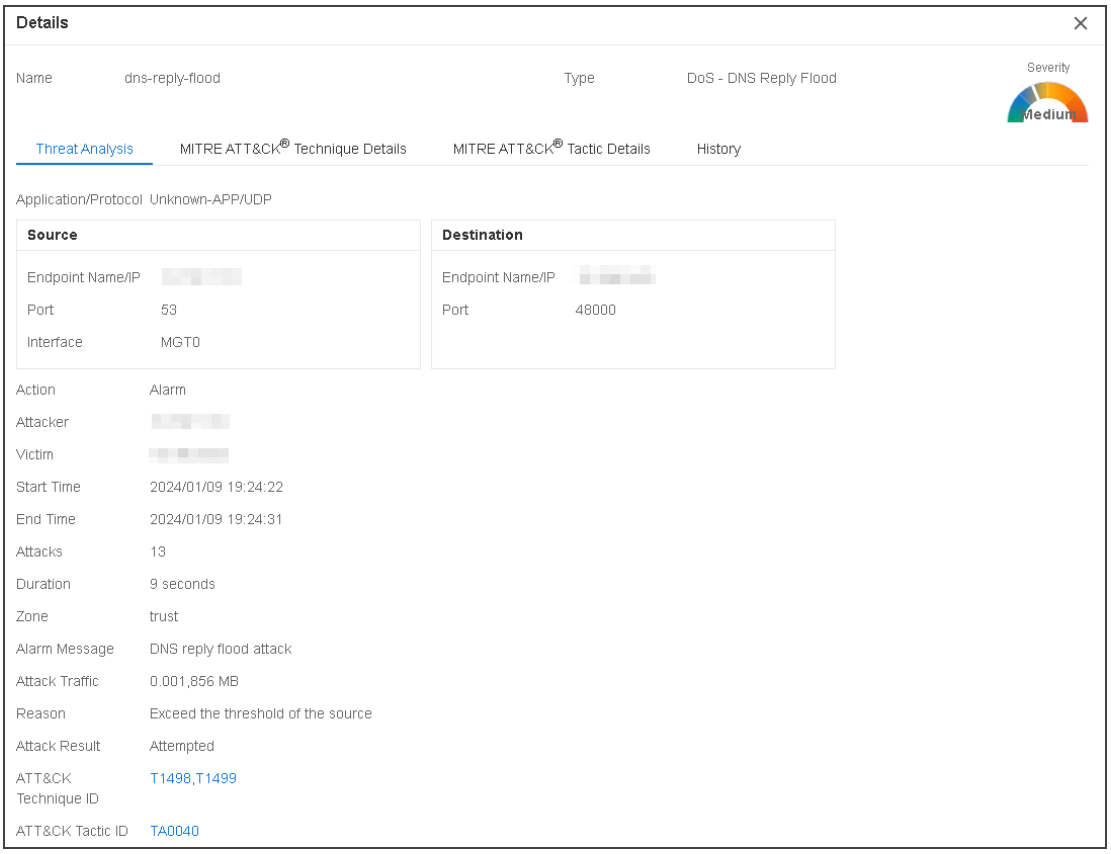
- Click the threat intelligence icon (, or) behind the address in the "Source"/"Destination" column in the list to open the threat intelligence center (CloudVista) to view the threat intelligence.

- Threat Analysis: Depending on the threats of the different detection engine , the content of Threat Analysis tab is also different.
    - **Anti Virus/IPS**: Display the detailed threat information .



For the Anti Virus/IPS function introduction, see /" Intrusion Prevention System" on Page 1315.

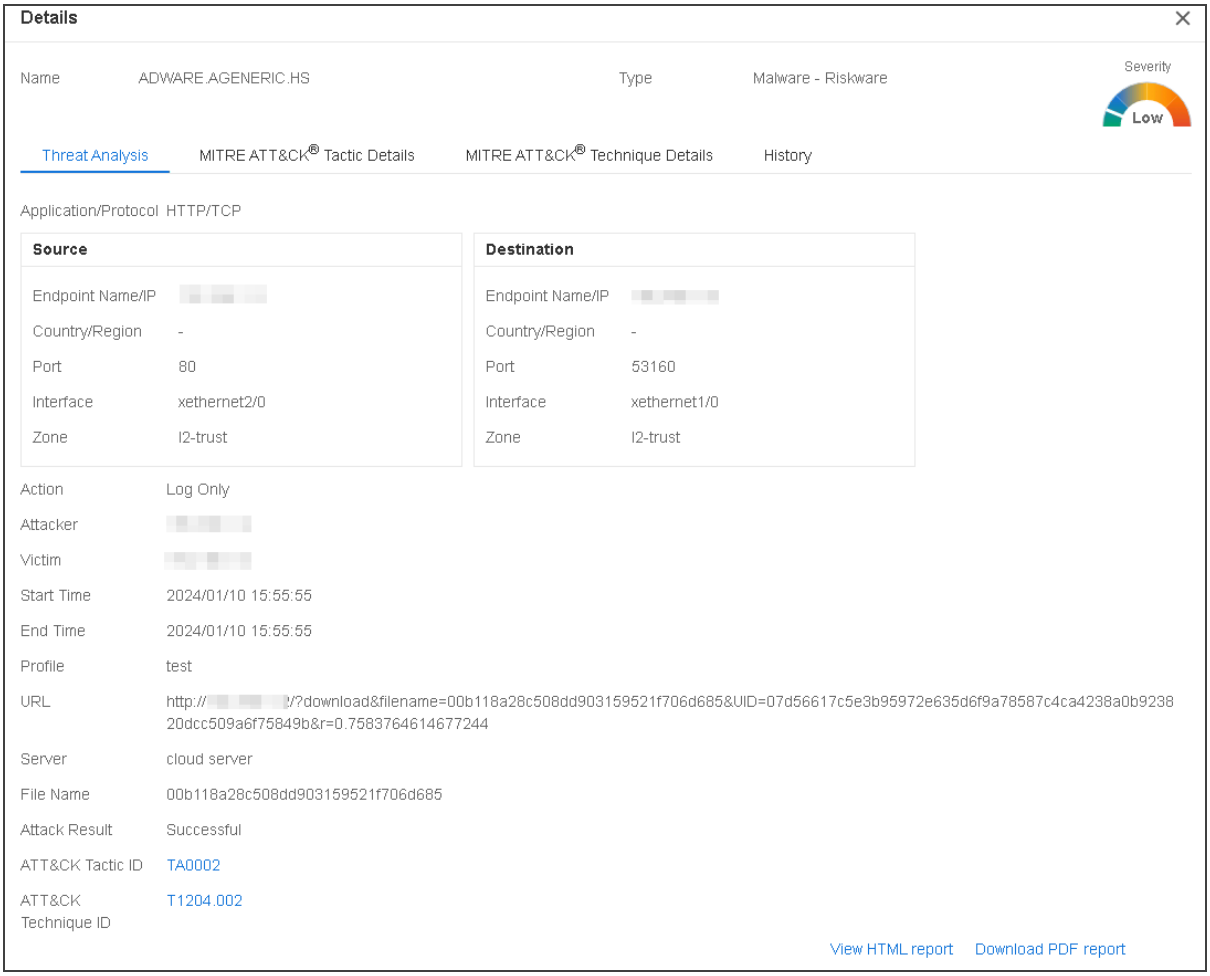
- **Attack Defense/Perimeter Traffic Filtering**: Display the threat detailed information.



Notes: Only details of flood attacks is supported to be displayed.

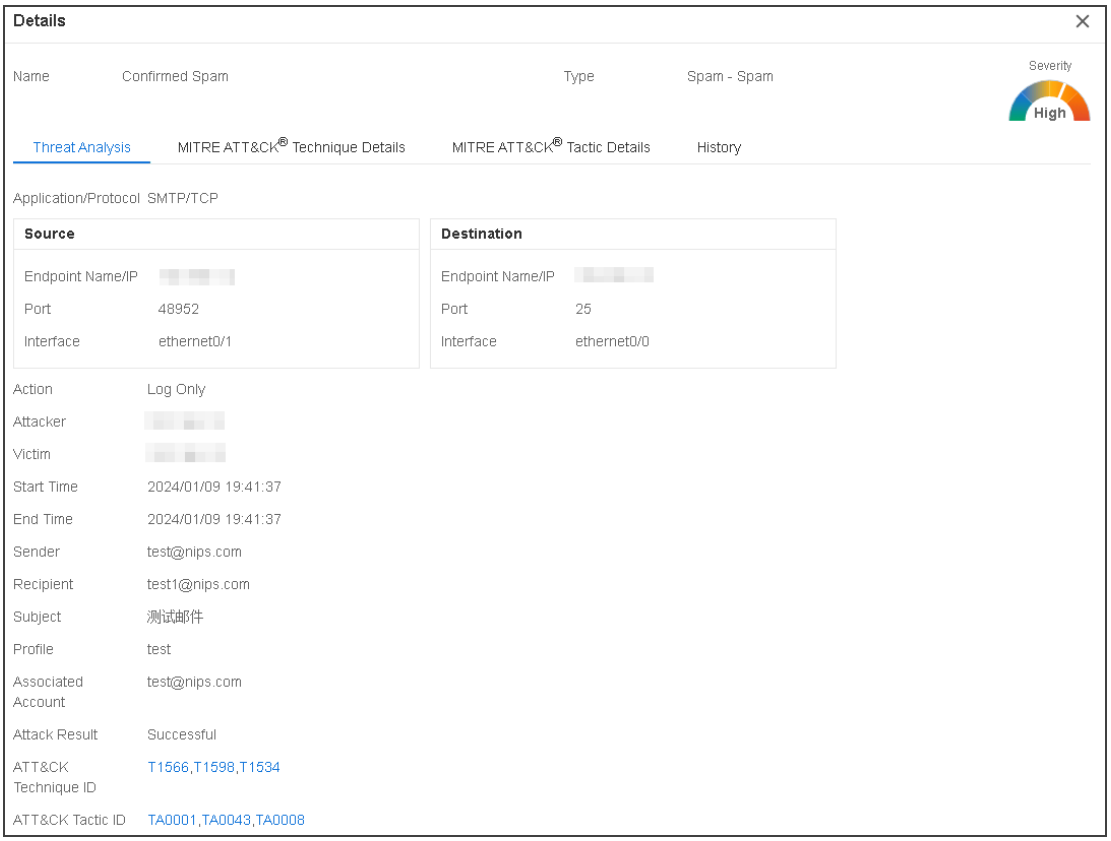
For the Attack Defense/Perimeter Traffic Filtering function introduction, see "Attack-Defense" on Page 1389/"Perimeter Traffic Filtering" on Page 1279.

- **Sandbox Threat Detection**: Display the detailed threat information of the suspicious file.



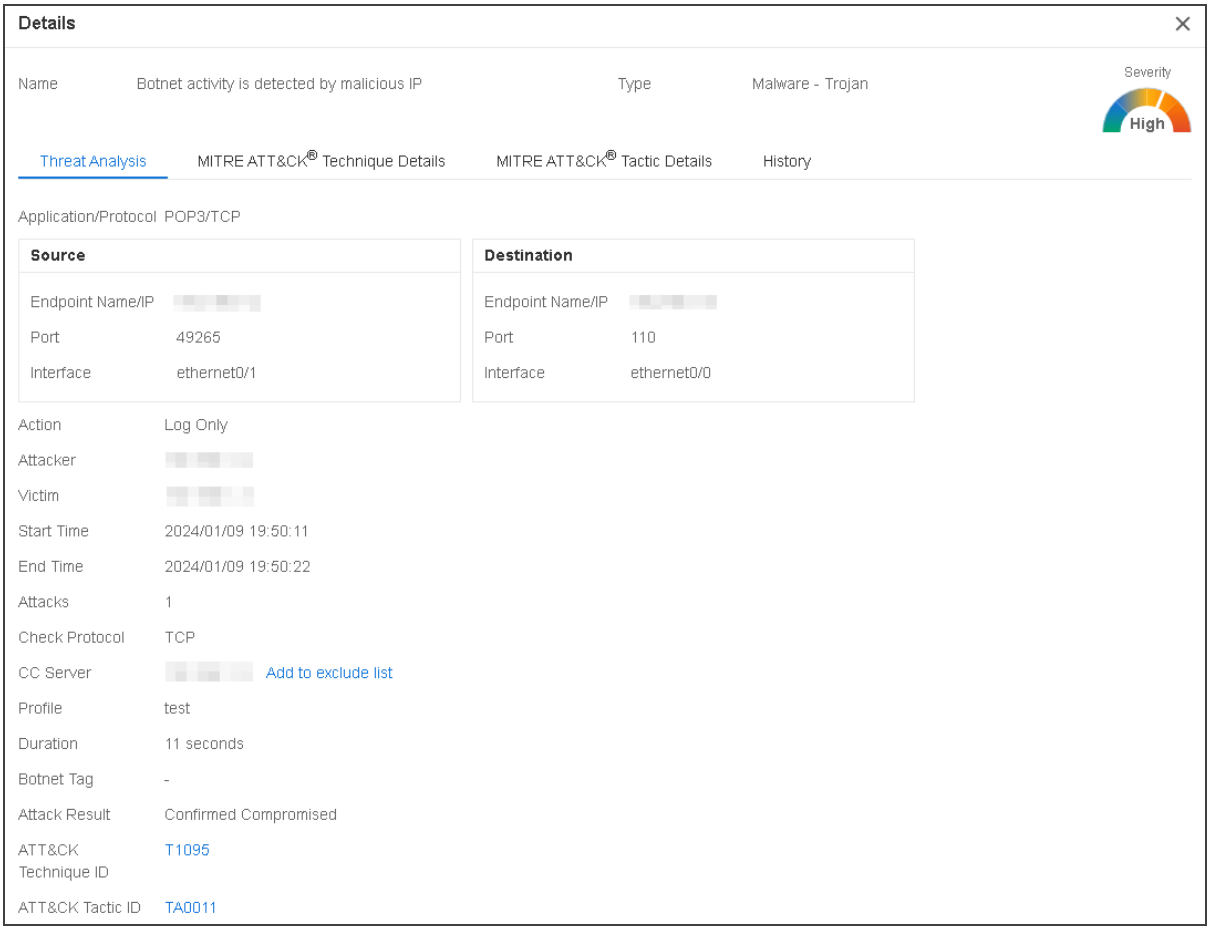
For the Sandbox function, see "Sandbox" on Page 1376.

- **Anti-Spam**:Display the spam filter information, such as sender and subject of spam.



For the Anti-Spam information, see "Antispam" on Page 1422.

- **Botnet Prevention**: Display the threat detailed information. If the threat is related to a malware family or APT group which is listed on the IOC blacklist, the system also displays the detailed information about the malware family or the APT group, including the Botnet tag.



For the Botnet Prevention information, see "Botnet Prevention" on Page 1429.

- Knowledge Base: Display the specified threat description, solution, etc. of the threats detected by IPS .
- MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base of attack behaviors. It categories known attacks as tactics and techniques, establishing a practical and clear framework. The system maps detected suspicious behaviors to the MITRE ATT&CK® model and displays the MITRE ATT&CK® tactic IDs and MITRE ATT&CK® technique IDs of the threat in threat logs, helping you identify suspicious behaviors in a better way. To ensure that the latest MITRE ATT&CK® knowledge base is used during detection, it is recommended to upgrade the MITRE ATT&CK® knowledge database. For more information about upgrading the MITRE ATT&CK®Knowledge Base, see Updating

Signature Database.

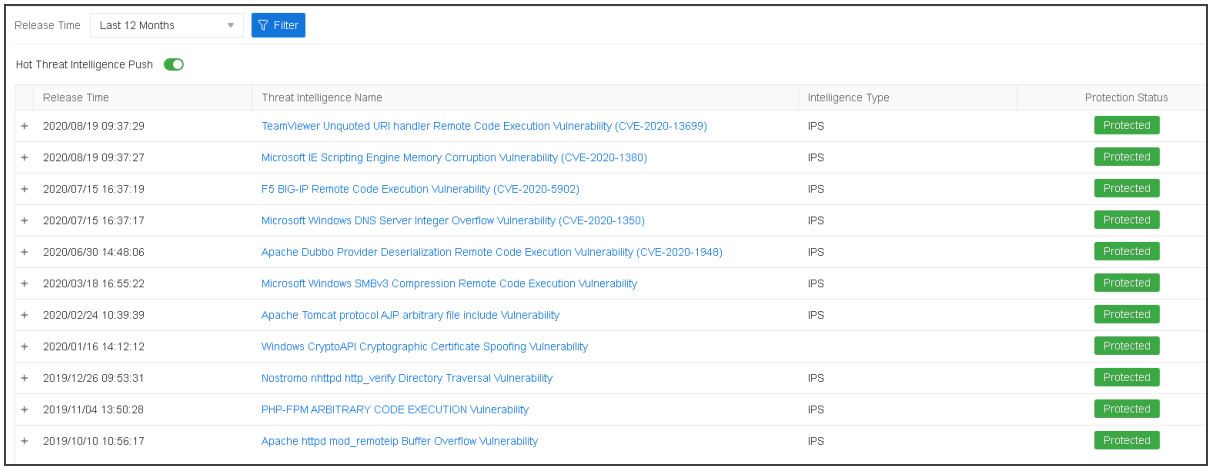
- **MITRE ATT&CK® Tactic Details**: MITRE ATT&CK® Tactic represents the tactical object of adversary and the reason for performing the attack. On the **MITRE ATT&CK® Tactic Details** tab, you can view the name, created time, last modified time, data source, official link, and description of this tactic.
- **MITRE ATT&CK® Technical Details**: MITRE ATT&CK® Technique represents how an adversary achieves a tactical goal by performing an action. On the **MITRE ATT&CK® Technical Details** tab, you can view this technique's name, data source, permission/system/network requirements, tactic, parent technique, sub technique, mitigation methods, official link, platform, etc.

- **Threat Data**: For threat events whose detection engine is IPS, if you have enabled the **Capture Threat Data** function, click **View** behind the **Threat Data** field. On the **Threat Data** panel, you can view ASCII and hex information of the threat. With the help of **Threat Data**, you can analyze the whole development process of the threat. If the **Capture Threat Data** function is disabled, the **Threat Data** section is not displayed on the **Details** panel. For more information about how to enable this function, refer to the **Configuring IPS** > **IPS Commands** topic in *StoneOS CLI User Guide*.
- Threat History: Display the selected threat historical information of the whole network .

Hot Threat Intelligence

Hot threat intelligence page displays the intelligence of hot threats on the Internet, including IPS vulnerability, virus and threats detected by the cloud sandbox. You can view the details of the hot threats, or carry out protection operations to prevent them.

Click **iCenter> Hot Threat Intelligence** to enter the Hot Threat Intelligence page. By default, the threats intelligence list shows the information of the latest year, including the release time, name, type, protection status and operation.



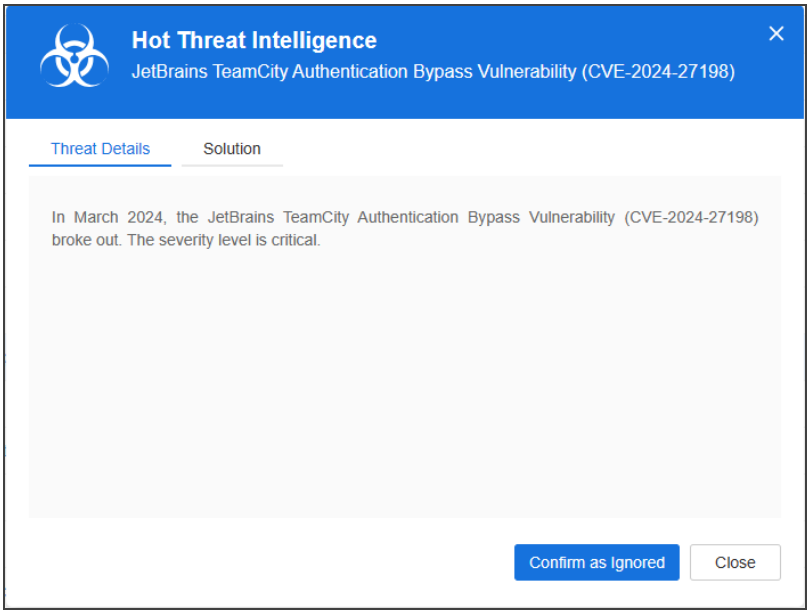
- Select a time period from the **Release Time** drop-down list to filter the threat information of the specified time period. Click + Filter to add conditions to filter threat information as needed.
- Click the button after "Hot Threat Intelligence Push". If it's enabled, Hillstone Cloud server will push the latest hot threat intelligence to system , and once system gets threat intelligence from the Hillstone Cloud server, it will be notified in the form of pop-up window. Otherwise, Hillstone cloud platform will no longer push the latest hot threat intelligence. Meanwhile, the previously received threat intelligence can only be viewed, and relevant protective operations are not allowed.
- Select one threat intelligence item in the list and the corresponding threat details and protection logs will be displayed below the list.
  - **Threat Details**: You can view the detailed threat information, including the release time ,the name, signature ID, severity, details, solutions, affected systems and other information (the items may vary slightly for different types of threat).

Option	Description
Release Time	Displays the release time of threat intelligence.
Threat Intel-	Displays the threat intelligence name.

Option	Description
ligence Name	
Signature ID	Displays the corresponded signature ID of the IPS signature database of the threat intelligence.
Severity	Displays the severity of threat intelligence.
Details	Displays the details of threat intelligence.
Solution	Displays the solutions to the threat .
Affected Sys-tems	Displays the name of operating system that the threat will affect.
CVE ID	Displays the CVE ID and link of the threat. Click the link address, and a new page will be opened, where you can view the CVE details.
Reference Information	Displays links of the reference information about the threat. Click the link address and a new page will be opened, where you can view details of the reference information.

- **Protection Log**: If system has been attacked by the threat described in the threat intelligence in the latest month, the protection logs will be displayed. If not, the protection log is empty.

- Click the threat intelligence name in the list or the corresponded operation ("Protect Now" or "View Details") in the "Operation" column, and the < Hot Threat Intelligence > dialog box will pop up. You can view the information about the hot threat intelligence in the dialog.



- Click <Threat Details> to view the information about the threat.
- For some threats in the "unprotected" status, you can see the corresponding protection solutions in the <Solution >tab. Click the links in sequence according to the steps in the solution, and configure the related functions. Only when you finish all the steps in one solutions (multiple solutions, at least one solution), the threat intelligence status will become "Protected". The description about each step button is as follows.
    a. Apply for License: apply for the corresponding Threat Prevention license.
    b. Reference Signature ID: associate a specified signature ID with the corresponding threat prevention function.
    c. Bind to Security Policy: configure the corresponding threat prevention function for the security policy.
    d. Bind to Zero-Trust Network Access Policy: configure the corresponding threat prevention function for the ZTNA policy.

e. Bind to Zone: configure the corresponding threat prevention function for the zone.

- For some threats in the "unprotected" status, the < Solutions> tab will not be displayed and you need to take the protective measures on other websites or servers, but system provides some solutions in the <Threats Details> tab. After the threat is protected, click **Confirm As Protected** button and the status of threat intelligence will be changed to "Protected".
- For some threats in the "unprotected" status, if you need to ignore a received hotspot threat intelligence, click **Confirm As Ignored**. This way, the status of this threat intelligence will be changed to "Ignored".

  Note: After the device restarts, "Ignored" threat intelligence will be recovered to a normal protection status ("Protected" or "Unprotected").
- For the threat in the "Protected" status, if it's protected by system, you can click < Protection List >to view the protective measures, and click "View Details" to view details of the protective measures.



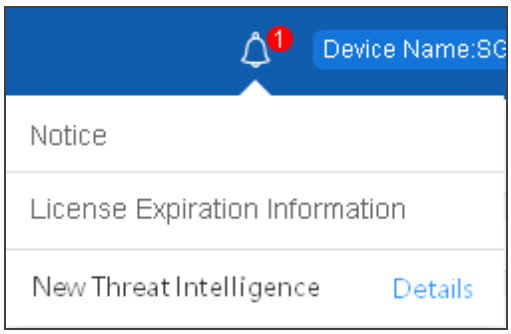
Notes: Because the operation steps in the < Solution >tab are correlated, please follow the steps of the solution in turn. For example, if the signature database has not been upgraded, the signature ID will not be shown, and subsequent protections may be unavailable. Or after the signature database is upgraded, the subsequent steps may change or some of the subsequent steps may be omitted.

Viewing Hot Threat Intelligence

System will obtain and download the latest threat intelligence information from the Hillstone cloud server at the set time every day or when you log in to system, and the information will be upgraded in the hot threat intelligence list.

When you enable the "Hot Threat Hot Threat Intelligence Push" function, once system gets a new intelligence, the notice of New Threat Intelligence will display in the upper right corner of

the page. Hover the mouse over the notification, click "details", and the page will jump to the hot threat intelligence page. On the **iCenter> Hot Threat Intelligence** page, the new threat intelligence will be displayed in the form of pop-up windows for users to view.



Chapter 5 Network

This chapter describes factors and configurations related to network connection, including:

- "Security Zone" on Page 152: The security zone divides the network into different section, such as the trust zone and the untrust zone. The device can control the traffic flow from and to security zones once the configured policy rules have been applied.
- "Interface" on Page 156: The interface allows inbound and outbound traffic flow to security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone.
- "Interface Group" on Page 239: The interface group function binds the status of several interfaces to form a logical group.
- "LLDP" on Page 240: LLDP (Link Layer Discovery Protocol) is a neighbor discovery protocol defined in IEEE 802.1ab, which provides a discovery method in link layer network.
- "Management Interface" on Page 248: To facilitate the management of the device and meet the requirement of separating the management traffic from the data traffic, system has an independent management interface(MGT Interface).
- "DNS" on Page 253: Domain Name System.
- "DHCP" on Page 270: Dynamic Host Configuration Protocol.
- "DDNS" on Page 284: Dynamic Domain Name Server.
- "PPPoE" on Page 288: Point-to-Point Protocol over Ethernet.
- "Virtual Wire" on Page 291: The virtual wire allows direct Layer 2 communications between sub networks.

- "Virtual Router" on Page 294: Virtual Routerouter (Virtual Router for short) acts as a router. Different Virtual Routers have their own independent routing tables.
- "Virtual Switch" on Page 296: Running on Layer 2, VSwitch acts as a switch. Once a Layer 2 security zone is bound to a VSwitch, all the interfaces bound to that zone will also be bound to the VSwitch.
- "Port Mirroring" on Page 298: Allow users to mirror the traffic of one interface to another interface (analytic interface) for analysis and monitoring.
- "WLAN" on Page 302: WLAN represents the local area network that uses the wireless channel as the medial. By configuring the WLAN function, you can establish the wireless local area network and allow the users to access LAN through wireless mode.
- "3G/4G" on Page 307: By configuring the 3G/4G function, users can access the Internet through the wireless mode.
- "Load Balancing " on Page 313: It takes advantage of dynamic link detection technique to assign traffic to different links appropriately, thus making full use of all available link resources.
- "Application Layer Gateway (ALG)" on Page 339: ALG can assure the data transmission for the applications that use multiple channels and assure the proper operation of VoIP applications in the strictest NAT mode.
- "Global Network Parameters" on Page 342: These parameters mainly include the IP packet's processing options, like IP fragmentation, TCP MSS value, etc.

Security Zone

Security zone is a logical entity. One or more interfaces can be bound to one zone. A zone applied with a policy is known as a security zone, while a zone created for a specific function is known as a functional zone. Zones have the following features:

- An interface should be bound to a zone. A Layer 2 zone will be bound to a VSwitch, while a Layer 3 zone will be bound to a VRouter. Therefore, the VSwitch to which a Layer 2 zone is bound decides which VSwitch the interfaces belong to in that Layer 2 zone, and the VRouter to which a Layer 3 zone is bound decides which VRouter the interfaces belong to in that Layer 3 zone.
- Interfaces in Layer 2 and Layer 3 are working in Layer 2 mode and Layer 3 mode respectively.
- System supports internal zone policies, like trust-to-trust policy rule.

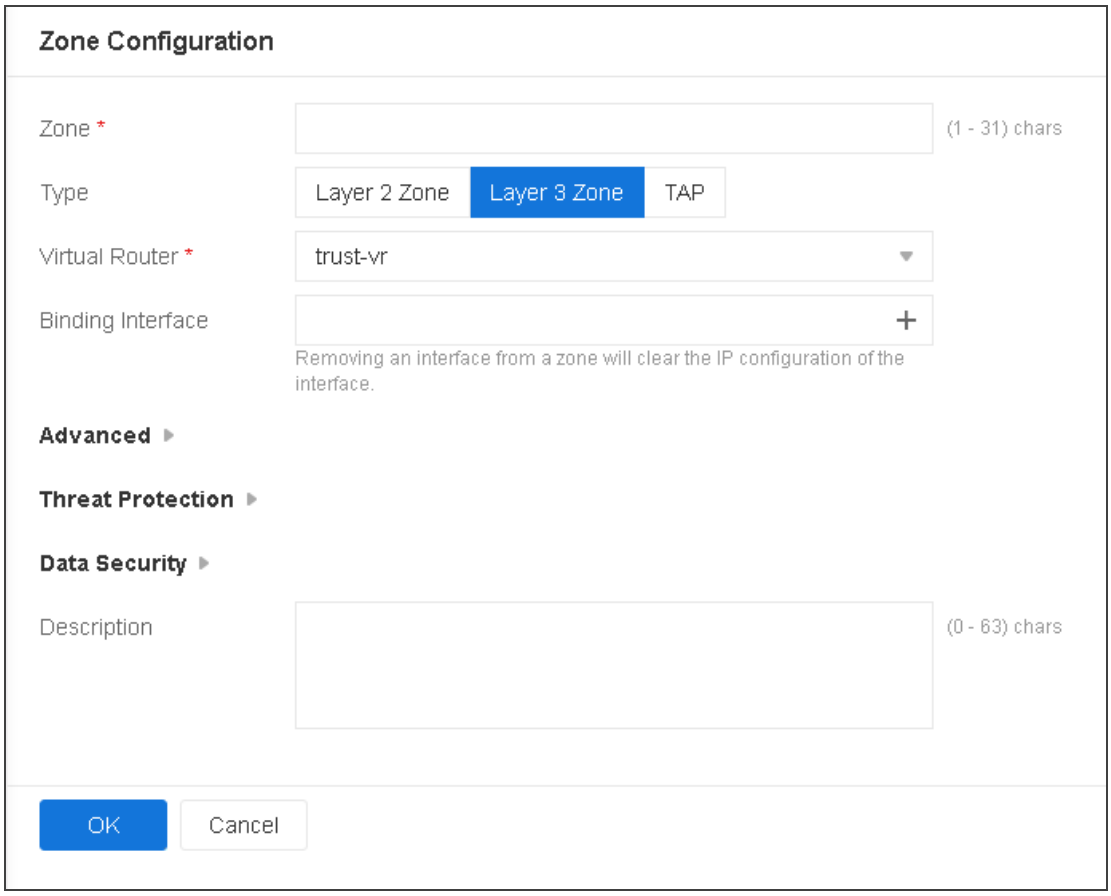
There are 8 pre-defined security zones in StoneOS, which are trust, untrust, dmz, L2-trust, L2-untrust, L2-dmz, vpnhub (VPN functional zone) and ha (HA functional zone). You can also customize security zones. Pre-defined security zones and user-defined security zones have no difference in functions, so you can make your choice freely.

Configuring a Security Zone

To create a security zone, take the following steps:

1. Select **Network > Zone**.

2. Click **New**.



3. In the Zone Configuration text box, type the name of the zone into the Zone box.

4. Type the descriptions of the zone in the Description text box.

5. Specify a type for the security zone. For a Layer 2 zone, select a VSwitch for the zone from the VSwitch drop-down list below; for a Layer-3 zone, select a VRouter from the Virtual Router drop-down list. If TAP is selected, the zone created is a tap zone, which is used in Bypass mode.

6. Bind interfaces to the zone. Select an interface from the Binding Interface drop-down list.

7. If needed, select the **Enable** button to enable APP identification for the zone.

8. If needed, select the **Enable** button to set the zone to a WAN zone, assuring the accuracy of the statistic analysis sets that are based on IP data.

9. If needed, select the **Enable** button to enable NetBIOS host query for the zone.

10. If needed, select Threat Protection tab and configure the parameters for Threat Protection function. For detailed instructions, see "Chapter 12 Threat Prevention" on Page 1299.

11. If needed, select Data Security tab and configure the parameters for Data Security function. For detailed instructions, see "Data Security" on Page 1018.

12. If needed, select End Point Prevention tab and configure the parameters for End Point Prevention function. For detailed instructions, see "End Point Protection" on Page 1452.

13. If needed, select IoT Monitor tab and configure the parameters for IoT Monitor function. For detailed instructions, see "IoT Monitor" on Page 1460.

14. Click **OK**.



Notes:

- Pre-defined zones cannot be deleted.
- When changing the VSwitch to which a zone belong, make sure there is no binding interface in the zone.
- The interface bound to the Tap zone only monitor the traffic but does not forward the traffic, but when the device enters the Bypass state (such as system restart, abnormal operation, and device power off), the Bypass interface pair will be physically connected, and then the traffic will be forwarded to each other. If you want to avoid this situation, try to avoid setting the pair of Bypass interfaces as the tap zone.

Interface

Interfaces allow inbound and outbound traffic to flow to security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone. Furthermore, for the Layer 3 security zone, an IP address should be configured for the interface, and the corresponding policy rules should also be configured to allow traffic transmission between different security zones. Multiple interfaces can be bound to one security zone, but one interface cannot be bound to multiple security zones.

Security gateway devices support various types of interfaces which are basically divided into physical and logical interfaces based on the nature.

- Physical Interface: Each Ethernet interface on devices represents a physical interface. The name of a physical interface, consisting of media type, slot number and location parameter, is pre-defined, like ethernet2/1 or ethernet0/2.
- Logical Interface: Include sub-interface, VSwitch interface, loopback interface, tunnel interface, aggregate interface, redundant interface, PPPoE interface, Virtual Forward interface, and Vif interface.

Interfaces can also be divided into Layer 2 interface and Layer 3 interface based on their security zones.

- Layer 2 Interface: Any interface in Layer 2 zone.
- Layer 3 Interface: Any interface in Layer 3 zone. Only Layer 3 interfaces can operate in NAT/routing mode.

Different types of interfaces provide different functions, as described in the table below.

Type	Description
Sub-interface	The name of an sub-interface is an extension to the name of its original interface, like ethernet0/2.1. System supports the following types of sub-interfaces: Ethernet sub-interface, aggregate sub-interface and redundant sub-interface. An interface and its sub-interfaces can be

Type	Description
	bound to one single security zone, or to different zones.
VSwitch interface	A Layer 3 interface that represents the collection of all the interfaces of a VSwitch. The VSwtich interface is virtually the upstream interface of a switch that implements packet forwarding between Layer 2 and Layer 3.
Loopback interface	A logical interface. If only the security device with loopback interface configured is in the working state, the interface will be in the working state as well. Therefore, the loopback interface is featured with stability.
Tunnel interface	Only a Layer 3 interface, the tunnel interface acts as an ingress for VPN communications. Traffic flows into VPN tunnel through this interface.
Aggregate interface	Collection of physical interfaces that include 1 to 16 physical interfaces. These interfaces averagely share the traffic load to the IP address of the aggregate interface, in an attempt to increase the available bandwidth for a single IP address. If one of the physical interfaces within an aggregate interface fails, other physical interfaces can still process the traffic normally. The only effect is the available bandwidth will decrease.
Redundant interface	The redundant interface allows backup between two physical interfaces. One physical interface, acting as the primary interface, processes the inbound traffic, and another interface, acting as the alternative interface, will take over the processing if the primary interface fails.
PPPoE interface	A logical interface based on Ethernet interface that allows connection to PPPoE servers over PPPoE protocol.

Type	Description
Virtual Forward interface	In HA environment, the Virtual Forward interface is HA group's interface designed for traffic transmission.
Vif Interface	The Vif interface is a logical interface, which is used for the Multicast Service Reflection (MSR) function.

Configuring an Interface

The configuration options for different types of interfaces may vary. For more information, see the following instructions.

Both IPv4 and IPv6 address can be configured for the interface.

Creating a PPPoE Interface

Notes: Non-root VSYS does not support to create the PPPoE interface.

To create a PPPoE interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > PPPoE Interface**.

In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the PPPoE interface.
Description	Enter descriptions for the PPPoE interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind

Option	Description
	to a Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
IP Configuration	
User	Specifies a user name for PPPoE.
Password	Specifies PPPoE user's password.
Confirm Password	Enter the password again to confirm.
Idle interval	If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connections; if the interface requires Internet access, the system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 0.
Re-connect interval	Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 10,

Option	Description
	which means the function is disabled.
Set gateway information from PPPoE server as the default gateway route	With this selected check box, system will set the gateway information provided by PPPoE server as the default gateway route.
Advanced	In the Advanced page, configure advanced options for PPPoE, including: • Access Concentrator - Specifies a name for the concentrator. • Authentication - The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). • Netmask - Specifies a netmask for the IP address obtained via PPPoE. • Static IP - You can specify a static IP address and negotiate about using this address to avoid IP change. To specify a static IP address, type it into the box. • Distance - Specifies a route distance. The value range is 1

Option	Description
	to 255. The default value is 1. • Weight - Specifies a route weight. The value range is 1 to 255. The default value is 1. • Service - Specifies allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, system will accept any service returned from the server automatically.
DDNS	In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF**, and **TRACEROUTE**.
WebAuth	
Auth Service	Click the **Enable**, **Close** or **Global Default** radio button as needed. • Enable: Enable the WebAuth function of the specified interface. • Close: Disable the WebAuth function of the specified interface.

Option	Description
	• Global Default: Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see "Web Authentication" on Page 470.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http://192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https://192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name

Option	Description
	instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

Expand Interface Properties, configure properties for the interface.

Option	Description
Parameters	
ARP Learning	Click the **Enable** button to enable ARP learning.
ARP Learning Limit	When a user host that connects to the interface initiates ARP attacks, ARP entry resources may be exhausted, making other interfaces unable to perform ARP learning. To avoid this issue, the system allows you to enable ARP learning limit and specify the maximum number of ARP entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ARP learning when the maximum number of ARP entries is reached. Click the button to enable ARP learning limit for the interface and enter the maximum number of ARP entries allowed on the interface. Valid values: 1 to capacity. **Note:** The capacity varies based on device platforms.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive packets.
MAC clone	System clones a MAC address in the Ethernet sub-interface. If

Option	Description
	the user click "Restore Default MAC", the Ethernet sub-interface will restore the default MAC address.
First Data Proxy	Turn on the switch to enable the First Data Proxy function. This way, the system can obtain and record domain information of HTTP/HTTPS packets in interface traffic. By default, this function is disabled.
HA VMAC	Specifies the custom HA MAC address. In the HA scenario, by default, the interface of HA master device forwards traffic with the virtual MAC address provided by system. You can configure a custom HA MAC address. In HA scenario, this custom HA MAC address is used for traffic forwarding of the master device. **Note:** • To ensure that the custom HA MAC takes effect, you need to enable the HA function. • The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local interface.
Mirror	Enable port mirroring on an Ethernet interface, and select the traffic type to be mirrored.
Bandwidth	
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Band-	Specifies the maximum value of the down bandwidth of the

Option	Description
width	interface.

Expand Advanced Configuration, configure advanced options for the interface.

Option	Description
NetFlow Configuration	Select a configured NetFlow profile from the drop-down list below.
Reverse Route	Enable or Disable reverse route as needed: • Enable: Force to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is to say, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Shutdown	System supports interface shutdown. You can not only force a specific interface to shut down, but also control the time it shuts down by schedule or according to the link status of tracked objects. Configure the options as below:

Option	Description
	1. Select the **Shut down** check box to enable interface shutdown. 2. To control the shutdown by schedule or tracked objects, select the appropriate check box, and then select an appropriate schedule or tracked object from the drop-down list or click ⊕ button to create a new schedule or a new track object.
Monitor and Backup	Configure the options as below: 1. Select the appropriate check box, and then select an appropriate schedule or tracked object from the drop-down list or click ⊕ button to create a new schedule or a new track object. 2. Select an action: • Shut down the interface: During the time specified in the schedule, or when the tracked object fails, the interface will be shut down and its related route will fail; • Migrate traffic to backup interface: During the time specified in the schedule, or when the tracked object fails, traffic flowing to the interface will be migrated to the backup interface. In such a case you need to select a backup interface

Option	Description
	from the Backup interface drop-down list and type the time into the Migrating time box. (Migrating time, 0 to 60 minutes, is the period during which traffic is migrated to the backup interface before the primary interface is switched to the backup interface. During the migrating time, traffic is migrated from the primary interface to the backup interface smoothly. By default the migrating time is set to 0, i.e., all the traffic will be migrated to the backup interface immediately.)

Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface.

Option	Description
Authentication mode	Specifies a packet authentication mode for the system, including plain text (the default) and MD5. The plain text authentication, during which unencrypted string is transmitted together with the RIP packet, cannot assure security, so it cannot be applied to the scenarios that require high security.
Authentication string	Specifies a RIP authentication string for the interface.
Transmit version	Specifies a RIP information version number transmitted by the interface. By default V1&V2 RIP information will be trans-

Option	Description
	mitted.
Receive version	Specifies a RIP information version number transmitted by the interface. By default V1&V2 RIP information will be transmitted.
Split horizon	Select the **Enable** checkbox to enable split horizon. With this function enabled, routes learned from an interface will not be sent from the same interface, in order to avoid routing loop and assure correct broadcasting to some extent.
Passive mode	The interface which receives data only but not send is known as a passive interface. Click the button to enable the interface as passive interface.

Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface.

Option	Description
Interface Timer	There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets. • Hello Transmission Interval: Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10. • Dead Time: Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello pack-

Option	Description
	ets). If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. • LSA Transmit Interval: Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5. • LSU Transmit Delay Time: Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1.
Priority	Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the designated router (The designated router will receive the link information of all the other routers in the network, and broadcast the received link information). If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.
Network Type	Specifies the network type of an interface. The network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast.

Option	Description
Link Cost	Click the **Enable** button to enable the link cost function. The value range is 1 to 65535. By default, the HA synchronization function is enabled, and the link cost will be synchronized to the backup device. Clear the check box to disable the synchronization function, and the system will stop synchronizing.

Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface.

Option	Description
Area ID	Specifies the area ID to which the interface belongs. The area ID is represented by 32 bits, which can be a number or an IP address.
Instance ID	Specifies the instance ID to which the interface belongs. The value range is 0 to 255. The default value is 0.
Interface Timer	There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets. • Hello Transmission Interval: Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10. • Dead Time: Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets). If a router has not received the Hello packet from its

Option	Description
	peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. • LSA Transmit Interval: Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5. • LSU Transmit Delay Time: Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1
Priority	Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the designated router (The designated router will receive the link information of all the other routers in the network, and broadcast the received link information). If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.
Link Cost	Specifies the link cost. The value range is 1 to 65535.
Passive	Some interfaces can be configured to receive updates but not send them. Such interfaces are passive interfaces. Click **Enable** to enable the passive interface.
MTU-Ignore	OSPFv3 uses DBD packets to check whether the MTU of inter-

Option	Description
	faces between neighbors match. If mtus of adjacent OSPFv3 router interfaces do not match each other, they cannot establish an adjacency relationship. You can modify the MTU of the interface to solve this problem. MTU cannot be modified on some interfaces. In this case, you can click the **Enable** button to make OSPFv3 ignore the MTU matching check.

Expand IPv6 Configuration, configure the following.

Option	Description
Enable	Enable IPv6 in the interface.
IPv6 Address	Specifies the IPv6 address prefix.
Prefix Length	Specifies the prefix length.
Autoconfig	Select the check box to enable Auto-config function. In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address. • Set Default Route - If the interface is configured with a default router, this option will generate a default route to the default router.
Enable DNS Proxy	Select this check box to enable DNS proxy for the interface.
DHCP	System supports DHCPv6 client, DHCPv6 server and DHCPv6 relay proxy. • Select **DHCP** check box to enable DHCP client for the

Option	Description
	interface. After enabling, system will act as a DHCPv6 client and obtain IPv6 addresses from the DHCP server. Selecting **Rapid-commit** option can help fast get IPv6 addresses from the server. You need to enable both of the DHCP client and the server's Rapid-commit function. • Select **DHCPv6 Server** from DHCP drop-down list and configure options as Configuring DHCPv6 Server, system will act as a DHCPv6 server to appropriate IPv6 addresses for DHCP client. • Select **DHCPv6 Relay Proxy** from DHCP drop-down list and configure options as Configuring DHCPv6 Relay Proxy, system will act as a DHCPv6 relay proxy to receive requests from a DHCPv6 client and send requests to the DHCPv6 server
IPv6 Advanced	
Static	Click Add button to add several IPv6 address, at most 5 IPv6 addresses.. Click Delete button to delete IPv6 address.
Dynamic	Shows IPv6 address which is dynamic.
Link-local	Specifies link-local address. Link-local address is used for communication between adjacent nodes of a single link. For example, communication between hosts when there are no routers on the link. By default system will generate a link-local address for the interface automatically if the interface is enabled

Option	Description
	with IPv6 (in the interface configuration mode, use the command ipv6 enable). You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one.
MTU	Specifies an IPv6 MTU for an interface. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
DAD Attempts	Specifies NS packet attempt times. The value range is 0 to 20. Value 0 indicates DAD is not enabled on the interface. If system does not receive any NA response packets after sending NS packets for the attempt times, it will verify that the IPv6 address is an unique available address. DAD (Duplicate Address Detection) is designed to verify the uniqueness of IPv6 addresses. This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving a NS packet, if any other host on the link finds that the address of the NS requester is duplicated, it will send a NA (Neighbor Advertisement) packet advertising that the address is already in use, and then the NS requester will mark the address as duplicate, indicating that the address is an invalid IPv6 address.

Option	Description
ND Learning	Click the button to enable ND learning for the interface. The interface obtains IP-MAC binding information in the internal network from ND learning and adds the binding information to the ND table. By default, ND learning is enabled. The interface continuously performs ND learning and adds the learned IP-MAC binding information to the ND table of the system. After the function is disabled, only IP addresses that are in the ND table can forward packets by using the interface.
ND Learning Limit	When a user host that connects to the interface initiates ND attacks, ND entry resources may be exhausted, making other interfaces unable to perform ND learning. To avoid this issue, the system allows you to enable ND learning limit and specify the maximum number of ND entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ND learning when the maximum number of ND entries is reached. Click the button to enable ND learning limit for the interface and enter the maximum number of ND entries allowed on the interface. Valid values: 1 to capacity. **Note:** The capacity varies based on device platforms.
ND Interval	Specifies an interval for sending NS packets.
ND Reachable Time	Specifies reachable time. After sending an NS packet, if the interface receives acknowledgment from a neighbor within the specified time, it will consider the neighbor as reachable. This time

Option	Description
	is known as reachable time.
Hop Limit	Specifies the hop limit. Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface.
ND RA Suppress	Select the checkbox to disable RA suppress on LAN interfaces. By default, FDDI interface configured with IPv6 unicast route will send RA packets automatically, and interfaces of other types will not send RA packets.
Manage IP/MASK	Specifies the manage IP/MASK.

3. Click **OK**.

Creating a Tunnel Interface



Notes: Non-root VSYS does not support to create the tunnel interface.

To create a tunnel interface:

1. Select **Network > Interface**.
2. Select **New > Tunnel Interface**.

In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the tunnel interface. The length varies from hardware platforms.
Description	Enter descriptions for the tunnel interface.

Option	Description
Binding Zone	If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
NetFlow configuration	Select a configured NetFlow profile from the drop-down list below.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses.  **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 270.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the

Option	Description
	gateway information provided by the DHCP server as the default gateway route. Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table.

Option	Description
	• MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU. **Notes:** • For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.) • By default, this function is disabled. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF** and **TRACEROUTE**.
Tunnel Binding	Bind the interface to a VPN tunnel or ZTNA instance. One tunnel interface can be bound to multiple IPSec VPN tunnels,

Option	Description
	while only to one SSL VPN tunnel. • IPSec VPN: Select IPSec VPN radio button. Specifies a name for the IPSec VPN tunnel that is bound to the interface. Then select a next-hop address for the tunnel, which can either be the IP address or the egress IP address of the peering tunnel interface. This parameter, which is 0.0.0.0 by default, will only be valid when multiple IPSec VPN tunnels is bound to the tunnel interface. • SSL VPN: Select SSL VPN radio button. Specifies a name for the SSL VPN tunnel that is bound to the interface.
TAP Configuration	• Control Interface: A bypass control interface is used to send control packets (TCP RST packet is supported in current version). After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, virus, or illegal network behaviors, it will send TCP RST packet from e2 to the switch to tell it to reset the connections. By default, the bypass control interface is the bypass interface itself. For tunnel interfaces, if the interface itself is used as the control interface, the control message sent by the tunnel interface may not be processed correctly. It is recommended that bypass tunnel interfaces be configured with other interfaces as control interfaces. When configuring, ensure

Option	Description
	that the control interface can send messages to the switch normally. • LAN Address: Specify a LAN address. Packets whose source IP is in the specified range will be counted.
Firewall Linkage Configuration	Specify the firewall information (firewall's IP, SSH port, login name, and password) in Firewall Linkage Configuration to combine the current device with a Hillstone firewall. If the device detects the attack traffic, it will send the IP of the attack source to the linkage firewall in the form of blacklist, and the linkage firewall will block the traffic of the attack source IP.
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Bandwidth	Specifies the maximum value of the down bandwidth of the interface.
Tunnel Binding: Bind VPN tunnel, IPv6 over IPv4 tunnel, or ZTNA instance to a tunnel interface. One tunnel interface can be bound to multiple IPSec VPN tunnels or GRE VPN tunnels, while only to one SSL VPN tunnel, one L2TP tunnel, one IPv6 over IPv4 tunnel, or one ZTNA instance.	
New	Click **New** to add an entry.
Type	Specifies the type of the tunnel or instance bound to a tunnel interface.
Name	Specifies the name of VPN tunnel, IPv6 over IPv4 tunnel, or ZTNA instance bound to a interface.

Option	Description
	Note: If you specify the instance type bound to the tunnel interface is ZTNA, only "remote access ZTNA instance" can be selected.
Domain	Bind the domain name to the L2TP tunnel. If you bind the domain name, usernames without the domain name cannot dial up successfully. If you do not bind the domain name, LNS will omit the domain name of usernames when authenticating users.
IPv4/IPv6 Gateway	The next hop IP addresses can be specified to either IPv4 or IPv6 addresses. Only when GRE VPN is bound can next hop IP addresses.

3. Expand Interface Properties, configure properties for the interface.

Option	Description
Parameters	
MTU	Specifies a MTU for the interface. The value range is 1280 to 1500/1800 bytes (The max MTU may vary on different platforms). The default value is 1500. Specifies the MTU value. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.

Option	Description
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive packets.
MAC clone	System clones a MAC address in the Ethernet sub-interface. If the user click "Restore Default MAC", the Ethernet sub-interface will restore the default MAC address.
First Data Proxy	Turn on the switch to enable the First Data Proxy function. This way, the system can obtain and record domain information of HTTP/HTTPS packets in interface traffic. By default, this function is disabled.
HA VMAC	Specifies the custom HA MAC address. In the HA scenario, by default, the interface of HA master device forwards traffic with the virtual MAC address provided by system. You can configure a custom HA MAC address. In HA scenario, this custom HA MAC address is used for traffic forwarding of the master device. **Note:** • To ensure that the custom HA MAC takes effect, you need to enable the HA function. • The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local interface.
Mirror	Enable port mirroring on an Ethernet interface, and select the

Option	Description
	traffic type to be mirrored.
Bandwidth	
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Bandwidth	Specifies the maximum value of the down bandwidth of the interface.

4. Expand IPv6 Configuration, configure the following.

Option	Description
Enable	Enable IPv6 in the interface.
IPv6 Address	Specifies the IPv6 address prefix.
Prefix Length	Specifies the prefix length.
Autoconfig	Select the check box to enable Auto-config function. In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address. • Set Default Route - If the interface is configured with a default router, this option will generate a default route to the default router.
Enable DNS Proxy	Select this check box to enable DNS proxy for the interface.
DHCP	System supports DHCPv6 client, DHCPv6 server and DHCPv6 relay proxy.

Option	Description
	• Select **DHCP** check box to enable DHCP client for the interface. After enabling, system will act as a DHCPv6 client and obtain IPv6 addresses from the DHCP server. Selecting **Rapid-commit** option can help fast get IPv6 addresses from the server. You need to enable both of the DHCP client and the server's Rapid-commit function. • Select **DHCPv6 Server** from DHCP drop-down list and configure options as Configuring DHCPv6 Server, system will act as a DHCPv6 server to appropriate IPv6 addresses for DHCP client. • Select **DHCPv6 Relay Proxy** from DHCP drop-down list and configure options as Configuring DHCPv6 Relay Proxy, system will act as a DHCPv6 relay proxy to receive requests from a DHCPv6 client and send requests to the DHCPv6 server.
IPv6 Advanced	
Static	Click Add button to add several IPv6 address, at most 5 IPv6 addresses.. Click Delete button to delete IPv6 address.
Dynamic	Shows IPv6 address which is dynamic.
Link-local	Specifies link-local address. Link-local address is used for communication between adjacent nodes of a single link. For example, communication between hosts when there are no routers on the link. By default system will generate a link-local

Option	Description
	address for the interface automatically if the interface is enabled with IPv6 (in the interface configuration mode, use the command ipv6 enable). You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one.
MTU	Specifies an IPv6 MTU for an interface. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
DAD Attempts	Specifies NS packet attempt times. The value range is 0 to 20. Value 0 indicates DAD is not enabled on the interface. If system does not receive any NA response packets after sending NS packets for the attempt times, it will verify that the IPv6 address is an unique available address. DAD (Duplicate Address Detection) is designed to verify the uniqueness of IPv6 addresses. This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving a NS packet, if any other host on the link finds that the address of the NS requester is duplicated, it will send a NA (Neighbor Advertisement) packet advertising that the address is already in use, and then the NS requester will mark the address as duplic-

Option	Description
	ate, indicating that the address is an invalid IPv6 address.
ND Interval	Specifies an interval for sending NS packets.
ND Reachable Time	Specifies reachable time. After sending an NS packet, if the interface receives acknowledgment from a neighbor within the specified time, it will consider the neighbor as reachable. This time is known as reachable time.
Hop Limit	Specifies the hop limit. Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface.
ND RA Suppress	Select the checkbox to disable RA suppress on LAN interfaces. By default, FDDI interface configured with IPv6 unicast route will send RA packets automatically, and interfaces of other types will not send RA packets.
Manage IP/MASK	Specifies the manage IP/MASK.

5. "Expand Interface Properties, configure properties for the interface." on Page 183
6. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 167
7. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 168
8. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 170
9. Click **OK**.

Creating a Virtual Forward Interface

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To create a virtual forward interface, take the following steps:

1. Select **Network > Interface**.
2. Select **New > Virtual Forward Interface**.

In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the virtual forward interface.
Description	Enter descriptions for the virtual forward interface.
Binding Zone	If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses. **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 270.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gate-

Option	Description
	way information provided by the DHCP server as the default gateway route. Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table.

Option	Description
	• MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU. **Notes:** • For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.) • By default, this function is disabled. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF** and **TRACEROUTE**.
WebAuth	
Auth Service	Click the **Enable**, **Close** or **Global Default** radio button as

Option	Description
	needed. • Enable: Enable the WebAuth function of the specified interface. • Close: Disable the WebAuth function of the specified interface. • Global Default: Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see "Web Authentication" on Page 470.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port numbe is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http://192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https://192.168.3.1:44434 certification.

Option	Description
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

3. "Expand IPv6 Configuration, configure the following." on Page 172
4. "Expand Interface Properties, configure properties for the interface." on Page 183
5. "Expand Advanced Configuration, configure advanced options for the interface." on Page 165
6. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 167
7. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 168
8. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 170
9. Click **OK**.

Creating a Loopback Interface

To create a loopback interface, take the following steps:

1. Select **Network > Interface**.

2. Click **New > Loopback Interface**.

In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the loopback interface.
Description	Enter descriptions for the loopback interface.
Binding Zone	If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP:In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced:  **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 270.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced:  **Notes:**

Option	Description
	 • For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.) • By default, this function is disabled. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF** and **TRACEROUTE**.

3. "Expand IPv6 Configuration, configure the following." on Page 172
4. "Expand Interface Properties, configure properties for the interface." on Page 183
5. "Expand Advanced Configuration, configure advanced options for the interface." on Page 165
6. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 167

7. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 168
8. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 170
9. Click **OK**.

Creating an Aggregate Interface

To create an aggregate interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Aggregate Interface**.
3. **In this page, configure the following.**

Option	Description
Interface Name	Specifies a name for the aggregate interface.
Description	Enter descriptions for the aggregate interface.
Binding Zone	Specifies the zone type. If Layer 2 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 2 zone. If TAP is selected, the interface will bind to a tap zone. You can specify the IPv4 or IPv6 LAN addresses from the LAN Address drop-down menu. With this configured, the device can identify the intranet traffic, and display them in the Monitor. And you can also specify the firewall information (firewall's Pv4

Option	Description
	or IPv6 address, SSH port, login name, and password) in Firewall Linkage Configuration to make the current device link with a Hillstone firewall. When the current device is working in the TAP mode and this interface is the one that receives the mirror traffic, if one or more of the following configurations are made, the device will send the matched traffic information to the linkage firewall which will block the traffic: • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the IPS rule that referenced by the security policy is Block IP or Block service; • The source zone of the share access rule is the TAP zone with this interface bound, and the action of the share access rule is Block; • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the end point profile that referenced by the security policy is Block; • The zone of the perimeter traffic filtering is the TAP zone with this interface bound, and the action of the perimeter traffic filtering is Block IP. If No Binding is selected, the interface will not bind to any zone.

Option	Description
Zone	Select a security zone from the Zone drop-down list.

Aggregate mode	• Forced: Aggregates multiple physical interfaces to form an aggregate interface. These physical interfaces will share the traffic passing through the aggregate interface equally.
	• Enables LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are:
	  • System priority: Specifies the LACP system priority. The value range is 1 to 32768, the default value is 32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be.
	  • Max bundle: Specifies the maximum active interfaces. The value range is 1 to 16, the default value is 16. When the active interfaces reach the maximum number, the status of other legal interfaces will change to Standby.
	  • Min bundle: Specifies the minimum active interfaces. The value range is 1 to 8, the default value is

Option	Description
	1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the aggregation group will change to Standby automatically and will not forward any traffic.
HA sync	Click this button to enable HA sync function. The primary device will synchronize its information with the backup device.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced:  **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 270.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box being selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.

Option	Description
	• Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>Notes:
For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.)
By default, this function is disabled.
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284.
Tip: This function is available only when you edit the interface.</td></tr>
<tr><td>PPPoE</td><td>User: Specifies a user name for PPPoE.
Password: Specifies PPPoE user's password.
Confirm Password: Enter the password again to confirm.
Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.
Re-connect Interval: Specifies a re-connect interval (i.e., sys-</td></tr>
</table>

Option	Description	
	tem will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.	
	Set gateway information from PPPoE server as the default gateway route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.	
	Advanced	Access concentrator: Specifies a name for the concentrator.
		Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.
		Netmask: Specifies a netmask for the IP address obtained via PPPoE.
		Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box.
		Service: Specifies allowed service. The spe-

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>cified service must be the same with that provided by the PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically.</td></tr>
<tr><td></td><td>Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.</td></tr>
<tr><td></td><td>Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1.</td></tr>
</table>
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284.
Tip: This function is available only when you edit the interface.
</td></tr>
<tr><td>Management</td><td>Select one or more management method check boxes to configure the interface management method, including Telnet, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.</td></tr>
<tr><td>TAP Configuration</td><td>Control Interface: A bypass control interface is used to send control packets (TCP RST packet is supported in current version). After configuring IPS, AV, or network behavior control on the Hillstone device, if the device detects network intrusions, virus, or illegal network behaviors, it will send TCP RST packet from e2 to the switch</td></tr>
</table>

Option	Description
	to tell it to reset the connections. By default, the bypass control interface is the bypass interface itself. For tunnel interfaces, if the interface itself is used as the control interface, the control message sent by the tunnel interface may not be processed correctly. It is recommended that bypass tunnel interfaces be configured with other interfaces as control interfaces. When configuring, ensure that the control interface can send messages to the switch normally. • LAN Address: Specify a LAN address. Packets whose source IP is in the specified range will be counted.
Firewall Linkage Configuration	Specify the firewall information (firewall's IP, SSH port, login name, and password) in Firewall Linkage Configuration to combine the current device with a Hillstone firewall. If the device detects the attack traffic, it will send the IP of the attack source to the linkage firewall in the form of blacklist, and the linkage firewall will block the traffic of the attack source IP.
WebAuth	
Auth Service	Click the **Enable**, **Close** or **Global Default** radio button as needed. • Enable: Enable the WebAuth function of the specified interface. • Close: Disable the WebAuth function of the specified

Option	Description
	interface. • Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see "Web Authentication" on Page 470.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the

Option	Description
	URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

4. "Expand IPv6 Configuration, configure the following." on Page 172
5. "Expand Interface Properties, configure properties for the interface." on Page 183
6. "Expand Advanced Configuration, configure advanced options for the interface." on Page 165
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 167
8. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 168
9. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 170
10. Expand Load Balance, configure a load balance mode for the interface. "Flow-based" means enabling automatic load balance based on the flow. This is the default mode. "Tuple" means enabling load based on the source/destination IP, source/destination MAC, source/destination interface or protocol type of packet, or the combination of the selected items.
11. Click **OK**.

Creating a Redundant Interface

To create a redundant interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Redundant Interface**.
3. "In this page, configure the following." on Page 198
4. "Expand IPv6 Configuration, configure the following." on Page 172
5. "Expand Interface Properties, configure properties for the interface." on Page 183
6. "Expand Advanced Configuration, configure advanced options for the interface." on Page 165
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 167
8. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 168
9. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 170
10. Click **OK**.

Creating an Ethernet Sub-interface/an Aggregate Sub-interface/a Redundant Sub-interface

To create an ethernet sub-interface/an aggregate sub-interface/a redundant sub-interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Ethernet Sub-interface/Aggregate Sub-interface/Redundant Sub-interface**.
3. In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the virtual forward interface.
Description	Enter descriptions for the virtual forward interface.
Binding Zone	If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced:  **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 270.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.

Option	Description
	• Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that the system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
Notes:

For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.)
By default, this function is disabled.

DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284.
Tip: This function is available only when you edit the interface.
</td></tr>
<tr><td>PPPoE</td><td>
<table>
<tr><td>User: Specifies a user name for PPPoE.</td></tr>
<tr><td>Password: Specifies PPPoE user's password.</td></tr>
<tr><td>Confirm Password: Enter the password again to confirm.</td></tr>
<tr><td>Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.</td></tr>
<tr><td>Re-connect Interval: Specifies a re-connect interval (i.e., sys-</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td colspan="2">tem will try to re-connect automatically after being dis-connected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.</td></tr>
<tr><td colspan="2">Set gateway information from PPPoE server as the default gate-way route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.</td></tr>
<tr><td rowspan="5">Advanced</td><td>Access concentrator: Specifies a name for the concentrator.</td></tr>
<tr><td>Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.</td></tr>
<tr><td>Netmask: Specifies a netmask for the IP address obtained via PPPoE.</td></tr>
<tr><td>Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box.</td></tr>
<tr><td>Service: Specifies allowed service. The specified</td></tr>
</table>
</td></tr>
</table>

Option	Description
	service must be the same with that provided by the PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically. Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including **Telnet**, **SSH**, **Ping**, **HTTP**, **HTTPS**, **SNMP**, **NETCONF** and **TRACEROUTE**.
WebAuth	
Auth Service	Click the **Enable**, **Close** or **Global Default** radio button as needed. • Enable: Enable the WebAuth function of the specified interface. • Close: Disable the WebAuth function of the specified

Option	Description
	interface. • Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see "Web Authentication" on Page 470.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port number is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http://192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https://192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web

Option	Description
	authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

4. "Expand IPv6 Configuration, configure the following." on Page 172
5. "Expand Interface Properties, configure properties for the interface." on Page 183
6. "Expand Advanced Configuration, configure advanced options for the interface." on Page 165
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 167
8. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 168
9. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 170
10. Click **OK**.

Creating a VSwitch Interface

To create a VSwitch interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > VSwitch Interface**.
3. "In this page, configure the following." on Page 189
4. "Expand IPv6 Configuration, configure the following." on Page 172
5. "Expand Interface Properties, configure properties for the interface." on Page 183

6. "Expand Advanced Configuration, configure advanced options for the interface." on Page 165
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 167
8. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 168
9. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 170
10. Click **OK**.

Creating a Vif Interface

The Vif interface is a logical interface, which is used for the Multicast Service Reflection (MSR) function. On the Vif interface, you can configure the IGMP Join-group function to direct multicast traffic to the MSR device, and then convert the original multicast streams (S1, G1) into new multicast streams (S2, G2) based on the address mapping configured on the MSR device.

To create a Vif interface, take the following steps:

1. Select **Network > Interface**.
2. Click **New > Vif Interface**.

   In this page, configure the following.

Option	Description
Interface Name	Specifies a name for the Vif interface, which can only be vif1. You can configure only one vif interface.
Description	Enter descriptions for the Vif interface.
Binding Zone	If Layer 3 zone is selected, you should also select a security

Option	Description
	zone from the Zone drop-down list, and the interface will bind to a Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the Zone drop-down list.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
IP Configuraton	

Option	Description
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface, which cannot be 32 or 255.255.255.255, otherwise, the MSR function does not take effect.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 32 secondary IP addresses.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 270.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route. Advanced:

Option	Description
	• Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU. After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send

Option	Description
	MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU. **Notes:** • For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.) • By default, this function is disabled. DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Management	Select one or more management method check boxes to configure the interface management method, including SSH, Ping, HTTPS , SNMP, NETCONF, TRACEROUTE, HTTP, and Telnet.

3. "Expand Interface Properties, configure properties for the interface." on Page 183
4. "Expand Advanced Configuration, configure advanced options for the interface." on Page 165
5. "Expand IPv6 Configuration, configure the following." on Page 172

6. Select Network > Routing > PIM, click Interface Configuration to open the Interface page and configure the MSR function for the selected interface.

7. Click **OK**.

Editing an Interface

To edit an interface, take the following steps:

1. Select **Network > Interface**.

2. Select the interface you want to edit from the interface list and click **Edit**.

3. **In this page, configure the following.**

Option	Description
Interface Name	Specifies a name for the interface.
Description	Enter descriptions for the interface.
Binding Zone	Specifies the zone type. IfLayer 2 zone is selected, you should also select a security zone from the Zone drop-down list, and the interface will bind to a Layer 2 zone. If TAP is selected, the interface will bind to a tap zone. You can specify the IPv4 or IPv6 LAN addresses from the LAN Address drop-down menu. With this configured, the device can identify the intranet traffic, and display them in the Monitor. You can also specify the firewall information (firewall's IPv4 or IPv6 address, SSH port, login name, and password) in Firewall Linkage Configuration to make the current device link with a Hillstone firewall. When the current device is working in the TAP mode and this interface is the one that receives the mirror

Option	Description
	traffic, if one or more of the following configurations are made, the device will send the matched traffic information to the link-age firewall which will block the traffic: • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the IPS rule that referenced by the security policy is Block IP or Block service; • The source zone of the share access rule is the TAP zone with this interface bound, and the action of the share access rule is Block; • The source zone and destination zone in the security policy is the TAP zone with this interface bound, and the action of the end point profile that referenced by the security policy is Block; • The zone of the perimeter traffic filtering is the TAP zone with this interface bound, and the action of the perimeter traffic filtering is Block IP. If No Binding is selected, you should also select an aggregate interface/redundant interface: • Aggregate Interface: The interface you specified belongs to a aggregate interface. • Interface: Choose an aggregate interface which the

Option	Description
	aggregate interface belongs to from Interface drop-down list. • Port LACP priority: Port LACP priority determines the sequence of becoming the Selected status for the members in the aggregate group. The smaller the number is, the higher the priority will be. Link in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority. • Port timeout mode: The LACP timeout refers to the time interval for the members The system supports **Fast** (1 second) and **Slow** (30 seconds, the default value) waiting to receive the LACPDU packets. If the local member does not receive the LACPDU packet from its peer in three timeout values, the peer will be conclude as down, and the status of the local member will change from Active to Selected, and stop traffic forwarding. • Redundant Interface: This interface belongs to a redundant interface. Select that redundant interface from the Interface drop-down list. • None: This interface does not belong to any object.
Aggregate	• Forced: Aggregates multiple physical interfaces to form an

Option	Description

mode	aggregate interface. These physical interfaces will share the traffic passing through the aggregate interface equally.
	• Enables LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are:
	  • System priority: Specifies the LACP system priority. The value range is 1 to 32768, the default value is 32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be.
	  • Max bundle: Specifies the maximum active interfaces. The value range is 1 to 16, the default value is 16. When the active interfaces reach the maximum number, the status of other legal interfaces will change to Standby.
	  • Min bundle: Specifies the minimum active interfaces. The value range is 1 to 8, the default value is 1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the

Option	Description
	aggregation group will change to Standby automatically and will not forward any traffic.
Zone	Select a security zone from the Zone drop-down list.
IP Configuration	
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced:  **Notes:** The secondary IP address of the configured interface and the current IP address of the interface must be in different network segments.
	DHCP: In the DHCP Configuration page, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 270.
	DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284. Tip: This function is available only when you edit the interface.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default

Option	Description
	gateway route. Advanced: • Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specifies a priority for the DNS server. Except for static DNS servers, system can also obtain DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server in descending order of priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority is. The priority of static DNS servers is 20. • Classless Static Routes: Enable the classless static routing function via the DHCP options. When it is enabled, the DHCP client will send a request message with the Option121 (i.e., classless static routing option) to the server, and then the server will return the classless static route information. Finally, the client will add the classless static routing information to the routing table. • MTU: Enable the function of obtaining the server MTU.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>After the function is enabled, the DHCP client sends option 26 (interface MTU) to the server, which will send MTU to the client after receiving the request. Then, the client uses the received MTU as the interface MTU.
 Notes:
• For the same interface, you cannot obtain the server MTU and configure the interface maximum transmission unit (MTU) at the same time. (To configure the interface MTU, specify the MTU parameter in the interface field section.)
• By default, this function is disabled.
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284.
Tip: This function is available only when you edit the interface.</td></tr>
<tr><td>PPPoE</td><td>User: Specifies a user name for PPPoE.
Password: Specifies PPPoE user's password.
Confirm Password: Enter the password again to confirm.
Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td colspan="2">Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.</td></tr>
<tr><td colspan="2">Re-connect Interval: Specifies a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.</td></tr>
<tr><td colspan="2">Set gateway information from PPPoE server as the default gateway route: With this check box being selected, system will set the gateway information provided by PPPoE server as the default gateway route.</td></tr>
<tr><td rowspan="4">Advanced</td><td>Access concentrator: Specifies a name for the concentrator.</td></tr>
<tr><td>Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). Click an authentication method.</td></tr>
<tr><td>Netmask: Specifies a netmask for the IP address obtained via PPPoE.</td></tr>
<tr><td>Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change.</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><td></td><td>To specify a static IP address, type it into the box.</td></tr>
<tr><td></td><td>Service: Specifies allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, Hillstone will accept any service returned from the server automatically.</td></tr>
<tr><td></td><td>Distance: Specifies a route distance. The value range is 1 to 255. The default value is 1.</td></tr>
<tr><td></td><td>Weight: Specifies a route weight. The value range is 1 to 255. The default value is 1.</td></tr>
</table>
DDNS: In the DDNS Configuration page, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 284.
Tip: This function is available only when you edit the interface.
</td></tr>
<tr><td>Management</td><td>Select one or more management method check boxes to configure the interface management method, including Telnet, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.</td></tr>
<tr><td colspan="2">WebAuth</td></tr>
<tr><td>Auth Service</td><td>Click the Enable, Close or Global Default radio button as needed.
Enable: Enable the WebAuth function of the specified</td></tr>
</table>

Option	Description
	interface. • Close：Disable the WebAuth function of the specified interface. • Global Default：Specify that the interface uses the global default configuration of WebAuth. For the global default configuration of WebAuth function, see "Web Authentication" on Page 470.
Proactive WebAuth	Click the **Enable** button to enable proactive webauth function and Specify the AAA server. After enabling, you can access the Web authentication address initiate authentication request, and then fill in the correct user name and password in the authentication login page. The Web authentication address consists of the IP address of the interface and the port number of the HTTP/HTTPS of the authentication server. For example the IP address of the interface is 192.168.3.1, authentication server HTTP/HTTPS port numbe is respectively configured as 8182/44434. When the authentication server is configured for HTTP authentication mode, Web address is: http:// 192.168.3.1:8182; when the authentication server is configured for HTTPS mode, the Web address for the https:// 192.168.3.1:44434 certification.
WebAuth Domain Name	Specifies the WebAuth domain name for the interface. The value range is from 1 to 255 characters.In passive WebAuth, you

Option	Description
	will be prompted to check the identity on the authentication page if you visit a service. In this case, if the Web authentication address is configured with a domain name, the URL of the Web authentication page will be displayed with the domain name instead of the IP address. Enable Web authentication before configuring the WebAuth domain name.

4. "Expand IPv6 Configuration, configure the following." on Page 172

5. Expand Interface Properties, configure properties for the interface.

Property	Description
Duplex	Specifies a duplex working mode for the interface. Options include auto, full duplex and half duplex. Auto is the default working mode, in which system will select the most appropriate duplex working mode automatically. 1000M half duplex is not supported.
Rate	Specifies a working rate for the interface. Options include Auto, 10M, 100M and 1000M. Auto is the default working mode, in which system will detect and select the most appropriate working mode automatically. 1000M half duplex is not supported. For 1GE(SFP) optical port of certain A-series devices, you can set the data rate to 100 Mbps or 1,000 Mbps. The default data rate is 1000 Mbps. When you set the data rate to 100 Mbps, the optical port can be inserted only into the 1GE (SFP) single-mode transceiver module and corresponding optical fibers. **Note**: Only the following devices allow you to backward switch

Property	Description
	the data rate of 1GE(SFP) optical port: SG-6000-A5500, A5200, A5100, A3800, A3700, A3600, A3000, A2800, and A2700.
Channel-Speed	Converts the data rate of 10GE (SFP+) optical interfaces. • 1G: Convert the data rate of 10GE (SFP+) optical interfaces from 10Gbps to 1Gbps. • Close: Do not convert the data rate of the 10GE (SFP+) optical interface, which is 10Gbps by default.
Combo type	This option is applicable to the Combo port of copper port + fiber port. If both the copper port and the fiber port are plugged with cable, the fiber port will be prioritized by default; if the copper port is used at first, and the cable is plugged into the fiber port, and the fiber port will be used for data transmission after reboot. You can specify how to use a copper port or fiber port. For detailed options, see the following instructions: • Auto: The above default scenario. • Copper forced: The copper port is enforced. • Copper preferred: The copper port is prioritized. • Fiber forced: The fiber port is enforced. • Fiber preferred: The fiber port is prioritized. With this option configured, the device will migrate the traffic on the copper port to the fiber port automatically without

Property	Description
	reboot.
MTU	The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.). If the Jumbo Frame function is enabled, the MTU value range is changed to 1280 bytes to 9300 bytes and the default MTU value is 1500 bytes. For more information about the Jumbo Frame function, see Configuring Global Network Parameters.
ARP Learning	Select the Enable checkbox to enable ARP learning.
ARP Learning Limit	When a user host that connects to the interface initiates ARP attacks, ARP entry resources may be exhausted, making other interfaces unable to perform ARP learning. To avoid this issue, the system allows you to enable ARP learning limit and specify the maximum number of ARP entries that can be learned on the interface. After a limit is specified, the interface can no longer perform ARP learning when the maximum number of ARP entries is reached. Click the button to enable ARP learning limit for the interface and enter the maximum number of ARP entries allowed on the interface. Valid values: 1 to capacity. **Note:** The capacity varies based on device platforms.
ARP Timeout	Specifies an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specifies an IP address that receives the interface's keep-alive

Property	Description
	packets.
MAC clone	System clones a MAC address to the Ethernet sub-interface. If the user click "Restore Default MAC", the Ethernet sub-interface will retore the default MAC address.
First Data Proxy	Turn on the switch to enable the First Data Proxy function. This way, the system can obtain and record domain information of HTTP/HTTPS packets in interface traffic. By default, this function is disabled.
HA VMAC	Specifies the custom HA MAC address. In the HA scenario, by default, the interface of HA master device forwards traffic with the virtual MAC address provided by system. You can configure a custom HA MAC address. In HA scenario, this custom HA MAC address is used for traffic forwarding of the master device. **Note**: • To ensure that the custom HA MAC takes effect, you need to enable the HA function. • The custom HA MAC address configuration does not take effect on the HA interface, loopback interface, and Local interface.
Bandwidth	
Up Bandwidth	Specifies the maximum value of the up bandwidth of the interface.
Down Band-	Specifies the maximum value of the down bandwidth of the

Property	Description
width	interface.

6. "Expand Advanced Configuration, configure advanced options for the interface." on Page 165
7. "Select Network > Routing > RIP, click Interface Configuration to open the <Interface> page and configure RIP for the selected interface." on Page 167
8. "Select Network > Routing > OSPF, click Interface Configuration to open the <Interface> page and configure OSPF for the selected interface." on Page 168
9. "Select Network > Routing > OSPFv3, click Interface Configuration to open the <Interface> page and configure OSPFv3 for the selected interface. " on Page 170
10. Click **OK**.



Notes:

- Before deleting an aggregate/redundant interface, you must cancel other interfaces' bindings to it, aggregate/redundant sub-interface's configuration, its IP address configuration and its binding to the security zone.
- An Ethernet interface can only be edited but cannot be deleted.
- When a VSwitch interface is deleted, the corresponding VSwitch will be deleted as well.
- The HA interface can not bind the track object.

Viewing the Interface Status

Select **Network** > **Interface**, you can view the status information of the interface in the **Interface Status** column of the interface list, and the status indicators are indicated as follows:

- Physical Status: Display the physical state of the interface. The icon indicates connected, the icon indicates HA keep up, the icon indicates disconnected or lacp disconnected.
- Management Status: Display the management state of the interface. The icon indicates connected, the icon indicates disconnected or lacp disconnected.
- Link Status: Display the link state of the interface. The icon indicates connected, the icon indicates HA keep up, the icon indicates disconnected or lacp disconnected.
- IPv4 Protocol Status (Only "Protocol Status" is displayed in the IPv4 version): Display the IPv4 protocol state of the interface. The icon indicates connected, the icon indicates HA keep up, the icon indicates disconnected or lacp disconnected.
- IPv6 Protocol Status (Only displayed in the IPv6 version): Display the IPv6 protocol state of the interface. The icon indicates connected, the icon indicates HA keep up, the icon indicates disconnected or lacp disconnected.

The interface list is displayed as follows:



Interface Name	Interface Status					Type	IP/Netmask	IPv6/Prefix	MAC
	Physical Statu	Management Status	Link Status	IPv4 Protocol Status	IPv6 Protocol Status				
aggregate1						IPv4: Static; IPv6: Static, Link-lo...	20.0.0.1/24	2001:1::1/128	001c.54fd.fa0b
aggregate2						IPv4: Static	0.0.0.0/0		001c.54fd.fa0c
aggregate3						IPv4: Static	0.0.0.0/0		001c.54fd.fa0d
tunnel1						IPv4: Static	192.100.100.1/24		001c.54fd.fa45
tunnel2						IPv4: Static	10.20.30.1/24		001c.54fd.fa46
tunnel3						IPv4: Static	0.0.0.0/0		001c.54fd.fa47
vswitchif1						IPv4: Static	0.0.0.0/0		001c.54fd.fa13
vswitchif2						IPv4: Static	0.0.0.0/0		001c.54fd.fa14

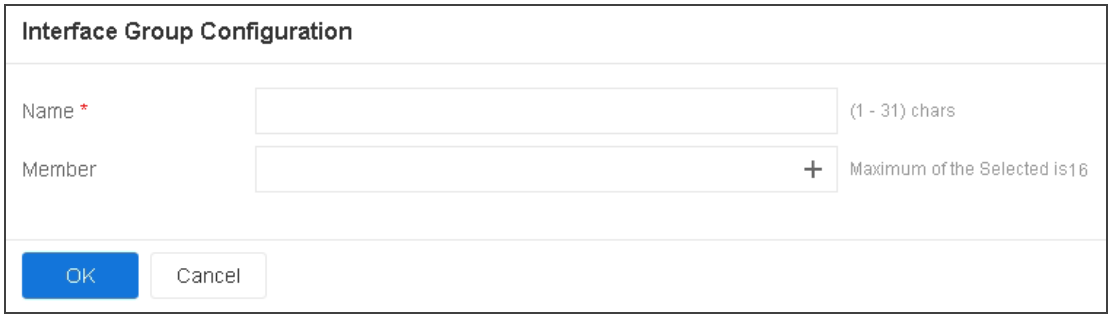
Interface Group

The interface group function binds the status of several interfaces to form a logical group. If any interface in the group is faulty, the status of the other interfaces will be down. After all the interfaces return to normal, the status of the interface group will be Up. The interface group function can binds the status of interfaces on different expansion modules.

Creating an Interface Group

To create an interface group, take the following steps:

1. Select **Network > Interface Group**.
2. Click **New**.



3. In the Interface Group Configuration page, type the name for the interface group. Names of the interface group can not be the same.
4. In the **Member** drop-down list, select the interface you want to add to the interface group. The maximum number of interfaces is 16.

   Note: Members of an interface group can not conflict with other interface groups.
5. Click **OK**.

   You can click **Edit** or **Delete** button to edit the members of interface group or delete the interface group.

LLDP

Network devices are increasingly diverse, and their configurations are respectively complicate. Therefore, mutual discovery and interactions in information of system and configuration between devices of different manufacturers are necessary to facilitate management. LLDP (Link Layer Discovery Protocol) is a neighbor discovery protocol defined in IEEE 802.1ab, which provides a discovery method in link layer network. By means of the LLDP technology, the system can quickly master the information of topology and its changes of the layer-2 network when the scale of network expands rapidly.

By means of LLDP, the LLDP information of the device, including the device information, system name, system description, port description, network management address and so on, can be sent in the form of standard TLV (Type Length Value) multicast message from the physical port to the directly-connected neighbor. If the neighbor enables LLDP too, then neighbor relations will be established between both sides. When the neighbor receives these messages, they are stored in the form of MIB in the SNMP MIB database, in order to be utilized by the network management system to search and analyze the two-layer topology and the problems in it of the current network.

LLDP Work Mode

The 4 work modes of LLDP are listed below:

- Transmit and Receive: the port transmits and receives LLDP messages.
- Receive only: the port only receives LLDP messages.
- Transmit only: the port only transmits LLDP messages.
- Not work: the port neither transmits nor receives LLDP messages.

Related links:

- Configuring LLDP
- Viewing MIB Topology

Configuring LLDP

Configuring LLDP can enable neighbor devices' collection of network topology changes.

- Enabling LLDP
- Modifying LLDP Configuration

Enabling LLDP

LLDP is enabled only when the "Global LLDP" and the "LLDP of Port" are enabled at the same time, so the corresponding port can transmit and receive LLDP messages.

- By default, the global LLDP and the LLDP of port are both disabled.
- When the global LLDP is enabled, the LLDP of port of all the ports of the system will be enabled.
- When the global LLDP is disabled, the LLDP of port of all the ports of the system will be disabled.
- When the global LLDP is enabled, the user does not have to modify LLDP configuration, for LLDP can be enabled by default configuration. If there is a need to optimize LLDP configuration, please see Modifying LLDP Configuration.

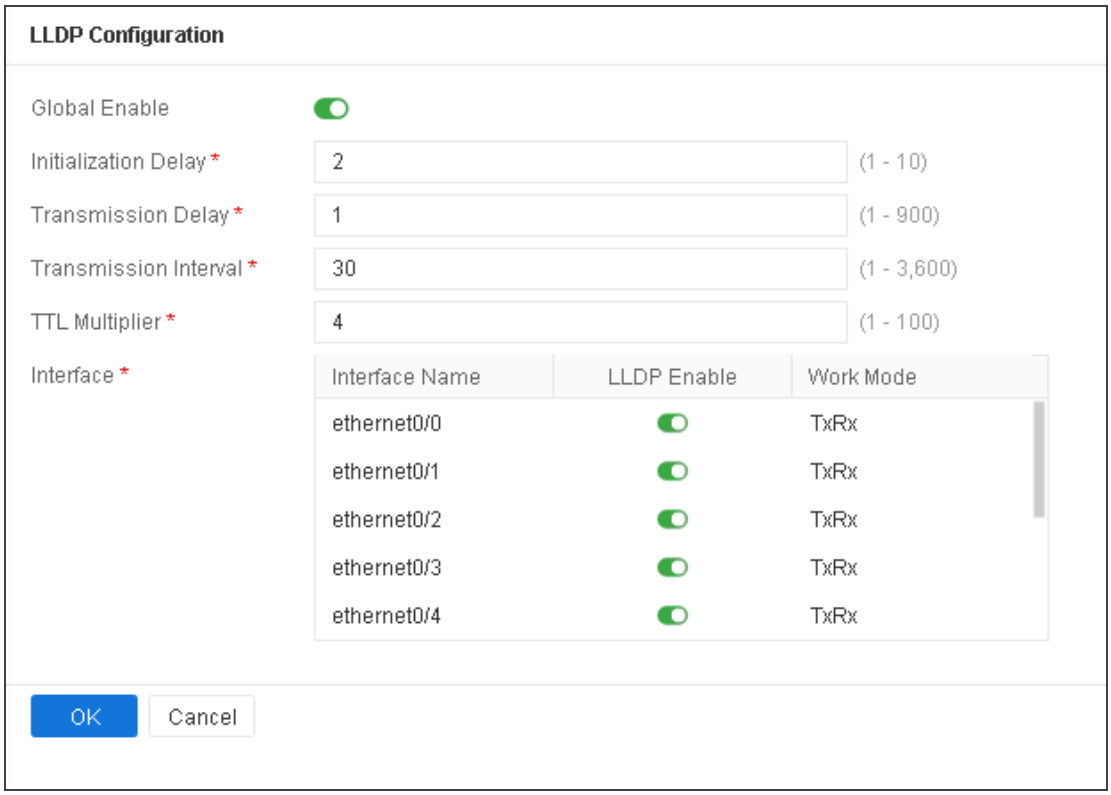


Notes: Only the physical port of the device supports enabling LLDP. Logical port does not support this function.

To enable the global LLDP, take the following steps:

1. Select **Network > LLDP > LLDP Configuration**.

2. Click **Global Enable** button.



3. Click **OK** to enable LLDP by default configuration.

   LLDP default configuration is as follows:

Option	Default
Initialization Delay	2 seconds
Transmission Delay	1 seconds
Transmission Interval	30 seconds

Option	Default
TTL Multiplier	4 seconds
port	LLDP is enabled in all the physical ports with the work mode being Transmit and Receive.

Modifying LLDP Configuration

According to the loading condition of network, the user can modify related LLDP configuration to reduce the consumption of system resources and optimize the LLDP performance.

To modify LLDP configuration, take the following steps:

- Select **Network > LLDP > LLDP Configuration**.

Option	Description
Initialization Delay	When the LLDP work mode of the port changes, the system will operate initialization on the port. Configuring the initialization delay of the port can avoid continuous initialization of the port due to frequent changes of the LLDP work mode. Type the delay time of initialization of the port in the **Initialization Delay** text box. The measurement is second-based, and the range is from 1 to 10.
Transmission Delay	Transmission delay refers to the minimal delay time before the LLDP messages are sent to the neighbor device when the state of the local device frequently changes. Type the minimal delay time before the LLDP message is sent in the **Transmission Delay** text box. The measurement is second-based, and the range is from 1 to 900.
Transmission Interval	Transmission interval refers to the time period of transmitting the LLDP message to the neighbor device when the state of the local device state remains stable. Type the transmission period before the LLDP message is sent in the **Transmission Interval** text box. The measurement is second-based, and the range is from 1 to 3600.
TTL Multiplier	TTL (Time to Live) refers to the living time of the local device information in the neighbor device. TTL multiplier is used to adjust the living time of the local device information in the neighbor device. The computational formula is: TTL = Transmission Interval × TTL Multiplier.

Option	Description
	Type the TTL multiplier value in the **TTL Multiplier** text box. The range is from 1 to 100.
port	Click the Enable button under **LLDP Enable** to enable the LLDP function of the port. Select LLDP work mode from the **Work Mode** drop-down menu to modify the LLDP work mode of the port. **Note**: For the introduction of the LLDP work mode, please see LLDP Work Mode.

- Click **OK**.

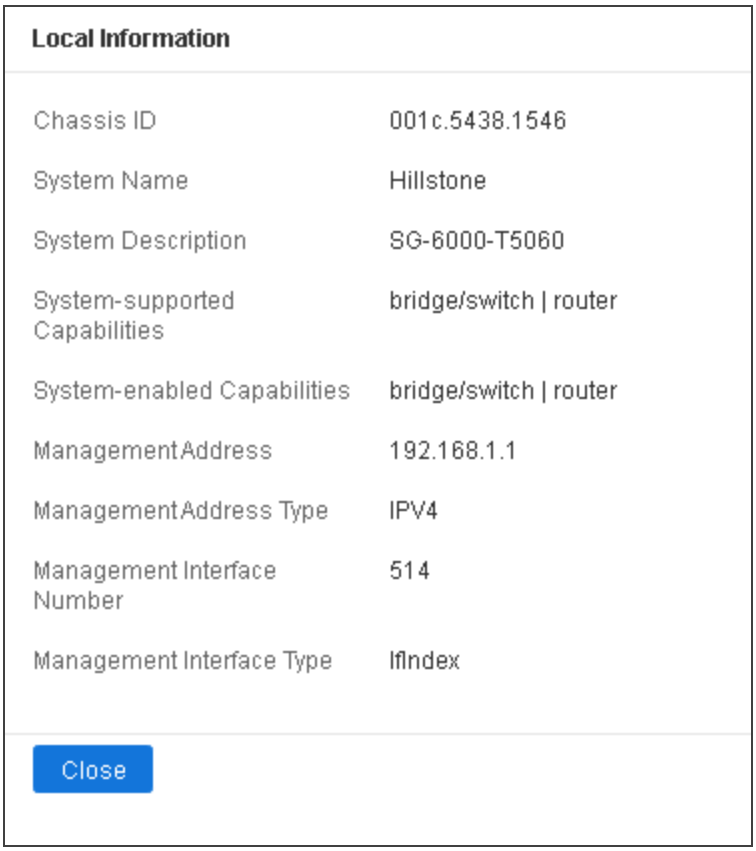
Viewing MIB Topology

The user can view the LLDP local information and the neighbor information (the LLDP information sent from the neighbor device to the local device) of the port in the **MIB Topology** page.

To view the MIB topology, take the following steps.

1. Select **Network > LLDP > MIB Topology**.
2. Click the **Local Information** button to open the **Local Information** page and view the LLDP local information, including chassis ID, system name, system description, system-supported

capabilities, management address and so on.



3. View the MIB topology and neighbor information of all the ports which enable LLDP in the list in the **MIB Topology** page.



Management Interface

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To facilitate the management of the device and meet the requirement of separating the management traffic from the data traffic, the system has an independent management interface (MGT Interface). By default, the management interface belongs to the mgt zone and the mgt-vr virtual router. The mgt zone belongs to the mgt-vr virtual router, the information of routing, ARP table are independent.

Configuring a Management Interface

To configure a MGT interface, take the following steps:

1. Select **Network > Management Interface**.
2. To edit a MGT interface, select the interface and click **Edit**, and the **MGT Interface** page pops up.

Option	Description
Interface Name	Show the name for the interface.
Zone	Specifies the zone for the management interface in the Zone drop-down list. You can only select a Layer 3 zone. By default, the interface is bound in the mgt zone.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the

Option	Description
	backup device.
NetFlow configuration	Select a configured NetFlow profile from the drop-down list below.
IP Configuration	
Static IP	IP address: Specifies an IP address for the interface.
	Netmask: Specifies a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specifies a management IP for the interface. Type the IP address into the box. • Secondary IP: Specifies secondary IPs for the interface. You can specify up to 10 secondary IP addresses.
	DHCP Server: Click the button to configure DHCP options for the interface in the DHCP Configuration page. For detailed instructions, see "DHCP" on Page 270.
Auto-obtain	Specifies to obtain the IP address through DHCP.
Management	Specifies the management methods by selecting the "Telnet/SSH/Ping/HTTP/HTTPS/SNMP" check boxes of the desired management methods.
Transmission Mode	Specifies the mode and rate of the management interface. If you select the Auto duplex transmission mode , you can only select

Option	Description
	the Auto rate.
Shut Down	Select the check box to shut down the management interface.

3. Expand IPv6 Configuration, configure the following.

Option	Description
Enable	Enable IPv6 in the interface.
IPv6 Address	Specifies the IPv6 address prefix.
Prefix Length	Specifies the prefix length.
Autoconfig	Select the check box to enable Auto-config function. In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address. • Set Default Route - If the interface is configured with a default router, this option will generate a default route to the default router.
DHCP	System supports DHCPv6 client and DHCPv6 server. • Select **DHCP** check box to enable DHCP client for the interface. After enabling, system will act as a DHCPv6 client and obtain IPv6 addresses from the DHCP server. Selecting **Rapid-commit** option can help fast get IPv6 addresses from the server. You need to enable both of the DHCP client and the server's Rapid-commit function.

Option	Description
	• Click the **DHCPv6 Server** button and configure options as Configuring DHCPv6 Server, system will act as a DHCPv6 server to appropriate IPv6 addresses for DHCP client.
IPv6 Advanced	
Static	Click Add button to add several IPv6 address, at most 5 IPv6 addresses. Click Delete button to delete IPv6 address.
Dynamic	Shows IPv6 address which is dynamic.
Link-local	Specifies link-local address. Link-local address is used for communication between adjacent nodes of a single link. For example, communication between hosts when there are no routers on the link. By default system will generate a link-local address for the interface automatically if the interface is enabled with IPv6 (in the interface configuration mode, use the command ipv6 enable). You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one.
MTU	Specifies an IPv6 MTU for an interface. The default MTU value is 1500 bytes. The range is 1280 bytes to 1800/2000 bytes (Different devices support different maximum MTU value.).
DAD Attempts	Specifies NS packet attempt times. The value range is 0 to 20. Value 0 indicates DAD is not enabled on the interface. If system does not receive any NA response packets after sending NS packets for the attempt times, it will verify that the IPv6 address is an

Option	Description
	unique available address. DAD (Duplicate Address Detection) is designed to verify the uniqueness of IPv6 addresses. This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving a NS packet, if any other host on the link finds that the address of the NS requester is duplicated, it will send a NA (Neighbor Advertisement) packet advertising that the address is already in use, and then the NS requester will mark the address as duplicate, indicating that the address is an invalid IPv6 address.
ND Interval	Specifies an interval for sending NS packets.
ND Reachable Time	Specifies reachable time. After sending an NS packet, if the interface receives acknowledgment from a neighbor within the specified time, it will consider the neighbor as reachable. This time is known as reachable time.
Hop Limit	Specifies the hop limit. Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface.
ND RA Suppress	Select the checkbox to disable RA suppress on LAN interfaces. By default, FDDI interface configured with IPv6 unicast route will send RA packets automatically, and interfaces of other types will not send RA packets.
Manage IP/MASK	Specifies the manage IP/MASK.

4. Click **OK**.

5. To create the virtual forward interface of MGT0 (that is, the MGT interface of HA group 1）, click **New** to open **Virtual Forward Interface** page for configuration.

DNS

DNS, the abbreviation for Domain Name System, is a computer and network service naming system in form of domain hierarchy. DNS is designed for TCP/IP network to query for Internet domain names (e.g., www.xxxx.com) and translate them into IP addresses (e.g., 10.1.1.1) to locate related computers and services.

The security device's DNS provides the following functions:

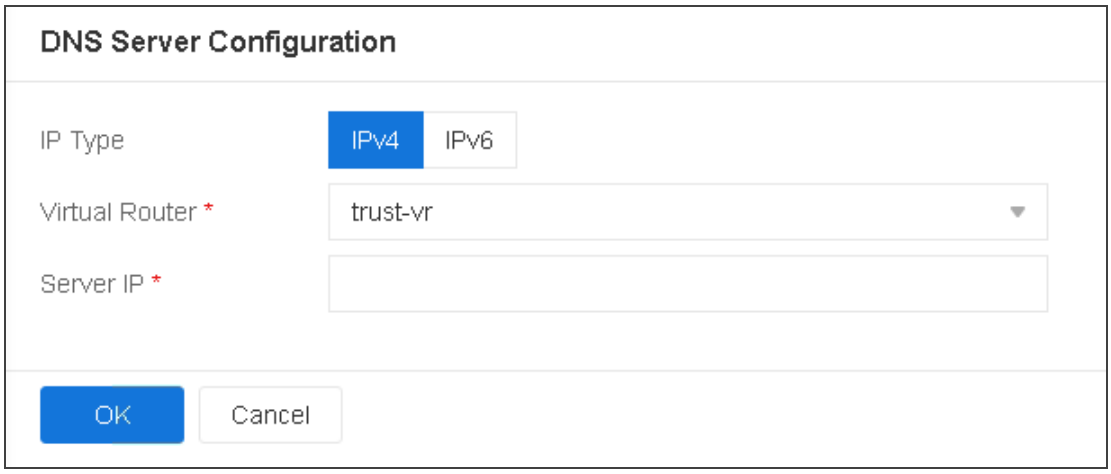
- Server: Configures DNS servers and default domain names for the security device.
- Proxy: As a DNS proxy, the device can filter the DNS request according to the DNS proxy rules set by the user, and system will forwarded the qualified DNS request to the designated DNS server.
- Analysis: Sets retry times and timeout for device's DNS service.
- Cache: DNS mappings to cache can speed up query. You can create, edit and delete DNS mappings.
- NBT Cache: Displays NBT cache information.

Configuring a DNS Server

You can configure a DNS server for system to implement DNS resolution. To create a DNS server, take the following steps:

1. Select **Network > DNS > DNS Server**.

2. Click **New** in the DNS Server section.



3. Select the IP address type, including IPv4 or IPv6.

4. Select a VRouter from the VR drop-down list. The default VRouter is trust-vr.

5. Type the IP address for the DNS server into the Server IP box

6. Click **OK**.

Configuring a DNS Proxy

DNS Proxy function take effect by the DNS proxy rules.Generally a proxy rule consists of two parts: filtering condition and action. You can set the filtering condition by specifying traffic's ingress interface, source address, destination address, and domain name. The action of the DNS proxy rules includes proxy, secure DNS, bypass, and block. When the action of the proxy rule is specified as proxy, you need to configure the DNS proxy servers, so that the DNS request meeting the filtering condition will be resolved by these DNS proxy servers.

Configuring a DNS Proxy Rule

To create a DNS proxy rule, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Click **New** in the DNS Proxy section.
3. In the <DNS Proxy Rule Configuration> page, configure the following settings.

Option	Description
Description	Add the description.
Type	Specify the type of a DNS proxy rule, IPv4 or IPv6.
Ingress Interface	Specify the ingress interface of DNS request in the rule to filter the DNS request message.It is permissible to specify numbers of interfaces.
Source Address	Specify the source address of DNS request to filter the DNS request message. It is permissible to specify multiple source address filtering conditions. Select the address entry type and then type the address. Click Add to add the selected entry to the pane. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close** to complete the source address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ button to create a new address entry.

Option	Description
	• You can click in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • When selecting the **IPv4** type, the default address configuration is any. To restore the configuration to this default one, select the **any** check box. • When selecting the **IPv6** type, the default address configuration is IPv6-any. To restore the configuration to this default one, select the **IPv6-any** check box.
Destination Address	Specify the destination address of DNS request to filter the DNS request message. It is permissible to specify multiple des-

Option	Description
	tination address filtering conditions. Select the address entry type and then type the address. Click Add to add the selected entry to the pane. 1. Select an address type from the **Address** drop-down list. 2. Select or type the destination addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close** to complete the destination address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click  button to create a new address entry. • You can click in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the

Option	Description
	addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • When selecting the **IPv4** type, the default address configuration is any. To restore the configuration to this default one, select the **any** check box. • When selecting the **IPv6** type, the default address configuration is IPv6-any. To restore the configuration to this default one, select the **IPv6-any** check box
Domain	Specify the domain name of DNS request to filter the DNS request message. It is permissible to specify multiple domain name filtering conditions. Select the domain entry type and then type the domain. Click **Add** to add the selected entry to the pane. 1. Select an address type from the **Domain** drop-down list. 2. Select or type the domain name. 3. Click **Add** to add the domain to the left pane. 4. After adding the desired domain, click **Close** to complete the domain configuration. You can also perform other operations:

Option	Description
	• When selecting the **Host Book** type, you can click **Add** to create a new host book entry. • The default domain configuration is any. To restore the configuration to this default one, select the **any** check box.
Action	Specify the action for a DNS proxy rule. For the DNS request that meets the filtering conditions, system can proxy, secure DNS, bypass, or block the traffic.
DNS Proxy Failed	Specify the action for DNS proxy failed. System can block or bypass the DNS request and then forward it to the DNS server originally requested by the message.
Log	Click the **Enable** button to enable the DNS proxy log function. With this function enabled, the system will generate log information when there is DNS request traffic matching this DNS proxy rule. You can view the DNS proxy log in the "Network Log" on Page 1571 page.
DNS Server	Specifies the DNS proxy server. When the action of the proxy rule is specified as Proxy, you need to configure the DNS proxy servers. You can specify up to six DNS servers for each DNS rule. You can customize the proxy server or specify a DNS server automatically obtained by the system. • When **User-defined** is selected, click **New** under the DNS server list and enter the IP address (IPv4 or IPv6 address)

Option	Description
	of the server and select the virtual router where the server belongs. You can bind the egress interface and preferred proxy as needed. When multiple DNS servers are configured, the preferred proxy server is given preference to resolve the domain. If no preferred server is specified, the system the system will query whether there are DNS servers that have specified the egress interface; If so, select these DNS server in a round robin. If there are only regular DNS server, then system will select this kind of DNS servers in a round robin. • When **Use System** is selected, select the virtual router or interface from the **Data Range** drop-down list to obtain the DNS server configured by the system or learned through a protocol, such as DHCP and PPPoE, from the specified virtual router or interface. **Note:** When the DNS server is configured as the IP address of the intranet DNS server, a DNS resolution dead loop may occur. Proceed with caution.
DNS64	If the IPv6 client host receives the DNS query request, it will use DNS64 to resolve the AAAA record (IPv6 address) in the DNS query information. If the resolution is successful, the IPv6 address is directly returned to the client. If the resolution fails, it will use DNS64 to resolve the A record (IPv4 address) in the DNS query information, and return the A record (IPv4 address) to the AAAA record (IPv6 address) to the client.

Option	Description
	Click the **Enable** button to enable the DNS64 function. By default, the DNS64 function is disabled.
DNS64 Server	The DNS64 server is used to resolve the A record (IPv4 address) in the DNS query information. Each IPv6 DNS proxy rule can specify up to 6 DNS64 servers. DNS64 Prefix: Specifies the DNS64 prefix and prefix length. The DNS64 prefix to synthesize the A record (IPv4 address) into an AAAA record (IPv6 address). The synthesized IPv6 address is in the form of "DNS64 prefix + IPv4 address". By default, the DNS64 prefix is "64:ff9b:: /96". At the bottom of the DNS64 server list, click the "+" button, and a table entry will be added. Enter the IP address (IPv4 address) of server and other parameters ,such as the virtual router.

4. Click **OK**.

Enabling/Disabling a DNS Proxy Rule

DNS proxy rule is enabled by default. To disable or enable the function, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Select the rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

Adjusting DNS Proxy Rule Position

To adjust the rule position, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Select the check box of the security policy whose position will be adjusted.
3. Click **Priority**.
4. In the pop-up menu, type the rule ID or name , and click **Top**, **Bottom**, **Before ID** , **After ID** , **Before Name** or **After Name**. Then the rule will be moved to the top, to the bottom, before or after the specified ID or name.

DNS Proxy Global Configuration

To set the DNS proxy global configuration, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Click **DNS Proxy Global Configuration** in the DNS Proxy section.
3. In the <DNS Proxy Global Configuration> page, configure the following settings.

Option	Description
TTL	Enable and specifies the TTL for DNS-proxy’ s response packets. If the DNS-proxy requests are not responded after the TTL, the DNS client will clear all DNS records. The value range is 30 to 600 seconds. The default value is 60.
Server Track	Enable the DNS proxy server track and configure the time interval of tracking for DNS proxy server. System will periodically detect the DNS proxy server at a specific time interval. When the server cannot be tracked, the IP address of server will be removed from the DNS resolution list untill the link is restored. By default, the tracking for DNS proxy server is enabled.
UDP Check-	Click the checkbox to enable/disable calculating the checksum

Option	Description
sum	of UDP packet for DNS proxy. The system will calculate the checksum of UDP packet for DNS proxy when the DNS proxy on interfaces is enabled. If you need to improve the performance of the device, you can disable this function.

4. Click **OK**.

DNS Proxy Hit Analysis

DNS Proxy Hit Analysis is a process to check the DNS proxy rule hit counts, that is, when DNS request traffic matches a certain DNS proxy rule, the hit count will increase by 1 automatically, and the ratio of the hit number of each DNS proxy rule to all the DNS requests of the system is counted, which directly shows the efficiency of the use of DNS proxy rules in the user network.

To view DNS proxy statistics, take the following steps:

1. Select **Network > DNS > DNS Proxy**.
2. Click **DNS Proxy Hit Analysis** above the DNS proxy rule list.

   View DNS proxy statistics in the <DNS Proxy Hit Analysis> page:

Option	Description
Time	Select a statistic period from the drop-down list: • Last 60 Minutes: Displays the statistical information within the latest 1 hour. • Last 24 Hours: Displays the statistical information within the latest 1 day. • Last 7 Days: Displays the statistical information within the latest 1 week.

Option	Description
	• Last 30 Days: Displays the statistical information within the latest 1 month. • All: Displays all the statistical information.
Clear	Click **Clear** to clear all the statistical information of all DNS proxy rules.
ID	Shows DNS proxy rule ID.
Hit count	Shows the hit count of a DNS proxy rule within the specified statistic period.
Hit percentage	Shows the ratio of the hit number of a DNS proxy rule to all the DNS requests of the system within the specified statistic period.

3. Click **Close**.

Configuring an Analysis

Analysis configuration includes DNS requests' retry times and timeout.

- Retry: If there is no response from the DNS server after the timeout, system will send the request again; if there is still no response from the DNS server after the specified retry times (i.e. the number of times to repeat the DNS request), system will send the request to the next DNS server.
- Timeout: System will wait for the DNS server's response after sending the DNS request and will send the request again if no response returns after a specified time. The period of waiting for a response is known as timeout.
- TTL: TTL refers to the survival time of the DNS domain name resolution cache (including dynamic DNS cache and register DNS cache). If the DNS resolution cache are not responded after the TTL, the system will clear all domain name records.

To configure the retry times, timeout and TTL for DNS requests, take the following steps:

1. Select **Network > DNS > Analysis**
2. Select the retry times radio button.
3. Select the timeout values radio button.
4. Turn on the switch next to **Interval Time** and specify the maximum interval for the device to send DNS requests to the DNS server in the **Max Interval Time** field. The value ranges from 60 to 3600 seconds. If not enabled, the device will send DNS requests to the DNS server after the domain name resolution cache has expired.

   
   Notes: This function takes effect only for register domain names.

5. Select the TTL radio button, which can be a value returned by DNS server (the default value) or a user-defined value (range from 60s to 86400s).
6. Click **Apply**.

Configuring a DNS Cache

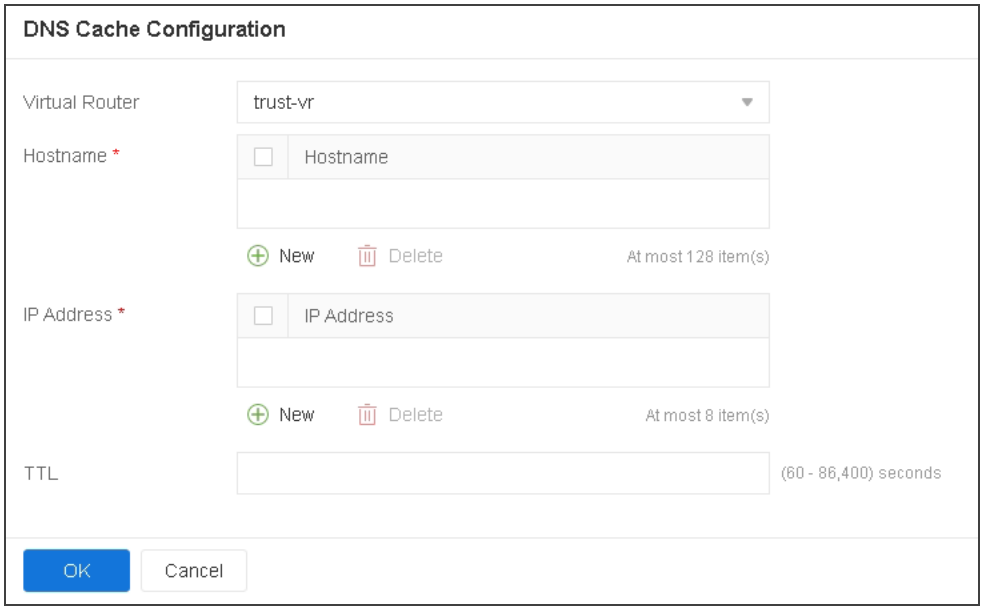
When using DNS, system might store the DNS mappings to its cache to speed up the query. There are three ways to obtain DNS mappings:

- Dynamic: Obtains from DNS response.
- Static: Adds DNS mappings to cache manually.
- Register: DNS hosts specified by some modules of security devices, such as NTP, AAA, etc.

For convenient management , DNS static cache supports group function, which means users make the multiple domain hosts with the same IP address and virtual router is a DNS static cache group.

To add a static DNS mapping to cache, take the following steps:

1. Select **Network > DNS > Cache**.
2. Click the IPv4 or IPv6 tab and configure the IPv4 or IPv6 DNS cache. This step applies only to the IPv6 version. If the device is in the IPv4 version, you can configure only the IPv4 DNS cache.
3. Click **New**.



Option	Description
Hostname	Specify the hostname of a DNS cache group. You can click ⊕ to add or click button to delete the specified hostname. The maximum number of domain hosts is 128, and the maximum length of each hostname is 255 characters.
IP	Specify the host IP address of a DNS cache group. You can click ⊕ to add or click button to delete the specified IP. The maximum number of host IP address is 8, and the earlier configured IP will be matched first.

Option	Description
Virtual Router	Select a VRouter.
TTL	Specify the TTL value, which is the duration that DNS cache group is retained on the device. When the device enables the DNS proxy function and the DNS request initiated by the client matches the DNS proxy rule, this TTL value is returned to the client if the DNS request hits the local cache. Valid values: 60 to 86400 seconds.

4. Click **OK**.



Notes:

- Only DNS static cache group can support new, edit and delete operation , while dynamic and register cache cannot .
- The DNS dynamic cache can be deleted by command or the lifetime reset. For detailed information , refer to **StoneOS CLI User Guide** and download PDF on website.
- User can clear the register cache only by deleting the defined hosts in function module.
- DNS static cache is superior to dynamic and register cache, which means the static cache will cover the same existed dynamic or register cache.

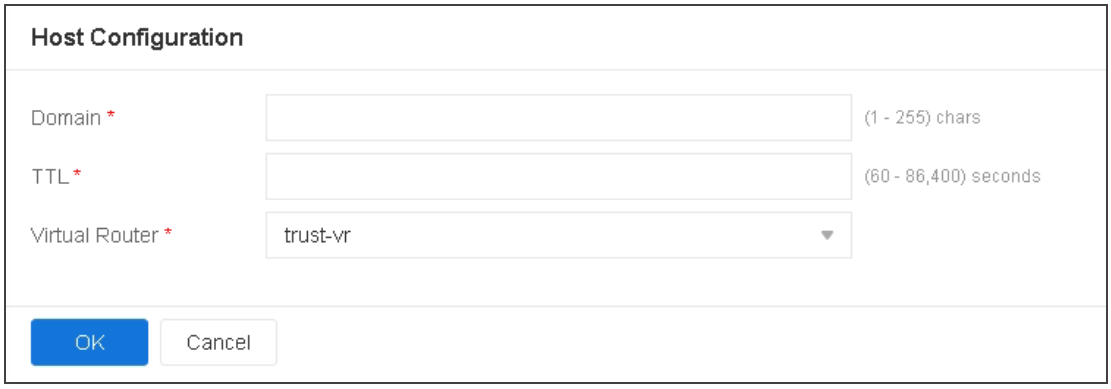
Configuring Host TTL

Host TTL refers to the survival time of the DNS domain name resolution cache, you can configure the TTL for the specified domain name resolution cache.

When the TTL value exceeds the specified value, the system sends a DNS request to the DNS server again. If a response is received, the cache is updated. If no response is received, the cache is cleared from the device.

To configure host TTL, take the following steps:

1. Select **Network** > **DNS** > **Host TTL Configuration**.
2. Click **New**.



Option	Description
Domain	Specifies the domain name, which ranges from 1 to 255 characters in length.
TTL	Specify the survival time of the DNS domain name resolution cache. The value range is 60 to 86400 seconds.
Virtual Router	Select a VRouter.

3. Click **OK**.

Notes:

- This function takes effect only for registered domain names. If you configure the TTL for dynamic or static domain names on this page, the configuration does not take effect.

- Host TTL has a higher priority than TTL of Configuring an Analysis.
- You can edit only the host TTL value, but not the domain name or virtual router.

NBT Cache

System supports NetBIOS name resolution. With this function enabled, system can automatically obtain all the NetBIOS host names registered by the hosts within the managed network, and store them in the cache to provide IP address to NetBIOS host name query service for other modules.

Enabling a NetBIOS name resolver is the pre-requisition for displaying host names in NAT logs. For more information on how to display host names in the NAT logs, see "Log Configuration" on Page 1602.

To enable NetBIOS for a zone, select the NBT cache check box when creating or editing the zone. For more details, see "Security Zone" on Page 152. The security zone with NetBIOS enabled should not be the zone that is connected to WAN. After NetBIOS is enabled, the query process might last for a while, and the query result will be added to the NetBIOS cache table. System will perform the query again periodically and update the result.

Notes: Only when PCs have NetBIOS enabled can their host names be queried. For more information on how to enable NetBIOS, see the detailed instructions of your PC's Operating System.

To clear NBT cache, take the following steps:

1. Select **Network > DNS > NBT Cache**.
2. Select a VRouter from the VR drop-down list to display the NBT cache in that VRouter.
3. Select a NBT cache entry from the list and click **Delete**.

DHCP

DHCP, the abbreviation for Dynamic Host Configuration Protocol, is designed to allocate appropriate IP addresses and related network parameters for subnetworks automatically, thus reducing requirement on network administration. Besides, DHCP can avoid address conflict to assure the re-allocation of idle resources.

DHCP supports to allocate IPv4 and IPv6 addresses.

System supports DHCP client, DHCP server and DHCP relay proxy.

- DHCP client: The interface can be configured as a DHCP client and obtain IP addresses from the DHCP server. For more information on configuring a DHCP client, see "Configuring an Interface" on Page 158.
- DHCP server: The interface can be configured as a DHCP server and allocate IP addresses chosen from the configured address pool for the connected hosts.
- DHCP relay proxy: The interface can be configured as a DHCP relay proxy to obtain DHCP information from the DHCP server and forward the information to connected hosts.

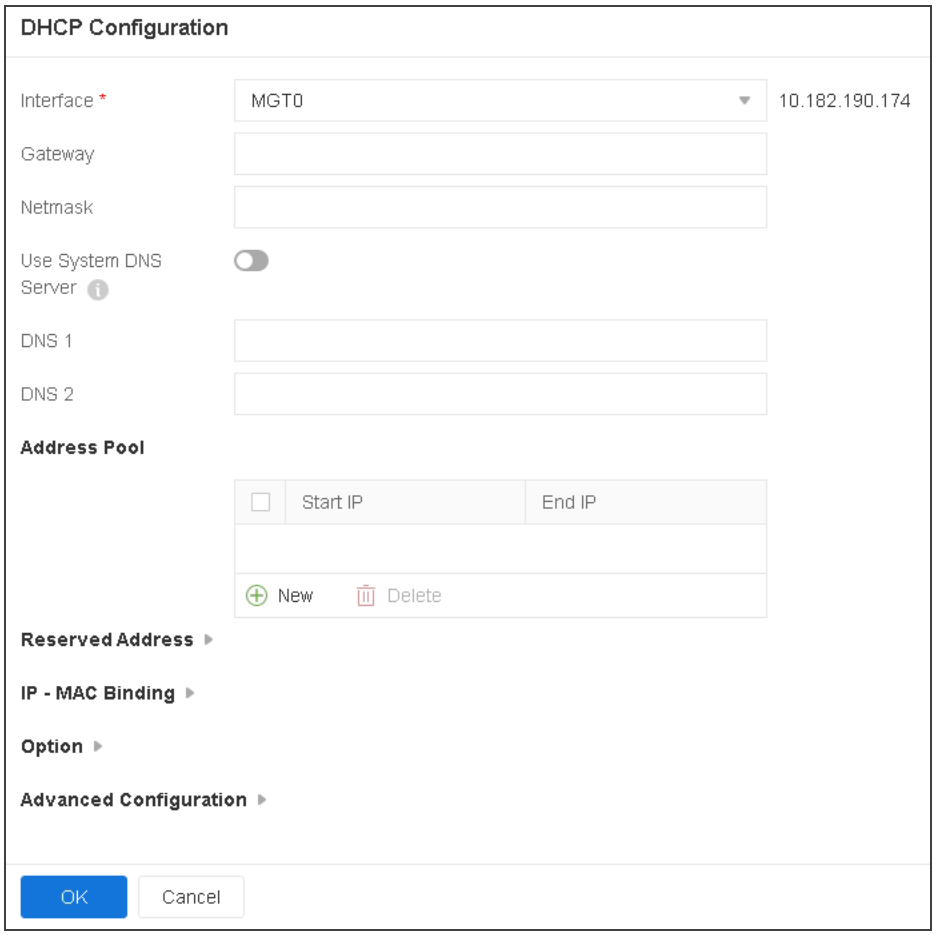
The security devices are designed with all the above three DHCP functions, but an individual interface can be only configured with one of the above functions.

Configuring a DHCP Server

To create a DHCP server, take the following steps:

1. Select **Network > DHCP**.

2. Select **New > DHCP Server**.



3. In the DHCP Configuration page, configure as following:

Option	Description
Interface	Configures a interface which enables the DHCP server.
Gateway	Configures a gateway IP for the client.
Netmask	Configures a netmask for the client.
Use System DNS Server	Click Enable. This way, the DNS server configured in the system is used as the DNS server of the client.

Option	Description
	Note: • If the system has configured more than two DNS servers, you can use the first two DNS servers as the DNS servers of the client; • After you enable Use System DNS Server, the system prioritizes providing DNS servers to the client by using this function.
DNS1	Configures a primary DNS server for the client. Type the server's IP address into the box.
DNS2	Configures an alternative DNS server for the client. Type the server's IP address into the box.
Address pool	Configures an IP range in the address pool. The IPs within this range will be allocated. Take the following steps: 1. Type the start IP and end IP into the Start IP and End IP box respectively. 2. Click **New** to add an IP range which will be displayed in the list below. 3. Repeat the above steps to add more IP ranges. To delete an IP range, select the IP range you want to delete from the list and click **Delete**.

4. Configure Reserved Address (IP addresses in the Reserved Address, within the IP range of the address pool, are reserved for the DHCP server and will not be allocated).
   To configure a reserved address, expand **Reserved Address**, type the start and end IP for an

IP range into the Start IP and End IP box respectively, and then click **New**. To delete an IP range, select the IP range you want to delete from the list and then click **Delete**.

5. Configure IP-MAC Binding. If the IP is bound to a MAC address manually, the IP will only be allocated to the specified MAC address.
   To configure an IP-MAC Binding, expand **IP-MAC Binding** and type the IP and MAC address into the IP address and MAC box respectively, type the description in the Description text box if necessary, and then click **New**. Repeat the above steps to add multiple entries. To delete an IP-MAC Binding, select an entry from the list and click **Delete**.

6. Expand Option, configure the options supported by DHCP server.

Option	Description
43	Option 43 is used to exchange specific vendor specific information (VSI) between DHCP client and DHCP server. The DHCP server uses option 43 to assign Access Controller (AC) addresses to wireless Access Point (AP), and the wireless AP use DHCP to discover the AC to which it is to connect. 1. Click **New**. 2. Select **43** from the **Option** drop-down list. 3. Select the type of the VSI, ASCII or HEX. When selecting ASCII, the VSI matching string must be enclosed in quotes if it contains spaces. 4. Enter the VSI in the **Sign** text box. **Notes:** If the VCI matching string has been configured, first of all, you need to verify the VCI

Option	Description
	carried by the option 60 field in client's DHCP packets. When the VCI matches the configured one, the IP address, option 43 and corresponding information will be offered. If not, DHCP server will drop client's DHCP packets and will not reply to the client.
49	After you configure the option 49 settings, the DHCP client can obtain the list of the IP addresses of systems that are running the X window System Display Manager. To configure the option 49 settings: 1. Click **New**. 2. Select **49** from the **Option** drop-down list. 3. Enter the IP address of the system that is running the X window System Display Manager into the **IP address** box. 4. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
60	After configuring the VCI carried by option 60 for DHCP server, the DHCP packets sent by the DHCP server will carry this option and the corresponding VCI. 1. Click **New**. 2. Select **60** from the **Option** drop-down list.

Option	Description
	3. Select the type of the VCI, ASCII or HEX. When selecting ASCII, the VCI matching string must be enclosed in quotes if it contains spaces. 4. Enter the VCI in the **Sign** text box. 5. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
66	The option 66 is used to configure the TFTP server name option. By configuring Option 66, the DHCP client get the domain name or the IP address of the TFTP server. You can download the startup file specified in the Option 67 from the TFTP server. 1. Click **New**. 2. Select **66** from the **Option** drop-down list. 3. Select the type of the TFTP server name, ASCII or HEX. When selecting ASCII, the length of TFTP server is 1 to 255 characters, but the maximum length between the two periods (.) is only 63 characters. 4. Enter the domain name or the IP address of the TFTP server in the **Sign** text box. 5. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
67	The option 67 is used to configure the startup file name option

Option	Description
	for the TFTP server. By configuring option 67, the DHCP client can get the name of the startup file. 1. Click **New**. 2. Select **67** from the **Option** drop-down list. 3. Select the type of the startup file name, ASCII or HEX. When selecting ASCII, the length of startup file name is 1 to 255 characters. 4. Enter the startup file name in the **Sign** text box. 5. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
138	The DHCP server uses option 138 to carry a list of 32-bit (binary) IPv4 addresses indicating one or more CAPWAP ACs available to the WTP. Then the WTP discovers and connects to the AC according to the provided AC list. 1. Click **New**. 2. Select **138** from the **Option** drop-down list. 3. Enter the AC IP address in the **IP address** text box. 4. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**. You can add up to four AC IP addresses. If you do not set the option 138 for the DHCP server or the DHCP client does not request option 138, DHCP server will

Option	Description
	not offer the option 138 settings.
150	The option 150 is used to configure the address options for the TFTP server. By configuring option 150, the DHCP client can get the address of the TFTP server. 1. Click **New**. 2. Select **150** from the **Option** drop-down list. 3. Enter the TFTP server IP address in the **IP address** text box. 4. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
242	The option 242 is a private DHCP private option for IP phones. By configuring option 242, the specific parameters information of IP phone can be exchanged between DHCP server and DHCP client, such as call server address (MCIPADD), call the server port (MCPORT), the address of the TLS server (TLSSRVR), HTTP (HTTPSRVR) HTTP server address and server port (HTTPPORT) etc. 1. Click **New**. 2. Select **242** from the **Option** drop-down list. 3. Select the type of the specific parameters of the IP phone, ASCII or HEX. When selecting ASCII, the length of startup file name is 1 to 255 characters.

Option	Description
	4. Enter the specific parameters of the IP phone in the **Sign** text box. 5. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.

7. Expand Advanced Configuration to configure the DHCP server's advanced options.

Option	Description
Domain	The domain name configured by the DHCP client.
Lease	Specifies a lease time. The value range is 300 to 1048575 seconds. The default value is 3600. Lease is the period during which a client is allowed to use an IP address, starting from the time the IP address is assigned. After the lease expires, the client will have to request an IP address again from the DHCP server.
Auto Configure	Enables automatic configuration. Select an interface with DHCP client enabled on the same gateway from the drop-down list. "----"indicates auto configure is not enabled. Auto configure will activate function in the following condition: Another interface with DHCP configured on the device enables DHCP client. When auto configure is enabled, if the DHCP server (Hillstone device) does not have DNS, WINS or domain name configured, the DHCP client (DHCP) will dispatch the DNS, WINS and domain name information obtained from a connected DHCP server to the host that obtains such information from the DHCP server (Hillstone device). However, the DNS, WINS and

Option	Description
	domain name that are configured manually still have the priority.
WINS1	Configures a primary WINS server for the client. Type the server's IP address into the box.
WINS2	Configures an alternative WINS server for the client. Type the server's IP address into the box.
Server	
SMTP server	Configures a SMTP server for the client. Type the server's IP address into the box.
POP3 server	Configures a POP3 server for the client. Type the server's IP address into the box.
News server	Configures a news server for the client. Type the server's IP address into the box.
Relay agent	When the device1 with DHCP server enabled is connected to another device2 with DHCP relay enabled, and the PC obtains device1's DHCP information from device2, then only when the relay agent's IP address and netmask are configured on device1 can the DHCP information be transmitted to the PC successfully. Relay agent: Type relay agent's IP address and netmask, i.e., the IP address and netmask for the interface with relay agent enabled on device2.
VCI-match-string	The DHCP server can verify the VCI carried by option 60 in the client’ s DHCP packets.When the VCI in the client's DHCP

Option	Description
	packet matches the VCI matching string you configured in the DHCP server, the DHCP server will offer the IP address and other corresponding information. If not, the DHCP server will drop the client's DHCP packets and will not reply to the client. If you do not configure a VCI matching string for the DHCP server, it will ignore the VCI carried by option 60. 1. Select the type of the VCI matching string, ASCII or HEX. When selecting ASCII, the VCI matching string must be enclosed in quotes if it contains spaces. 2. Enter the VCI matching string in the text box.

8. Click **OK**.

Configuring a DHCP Relay Proxy

The device can act as a DHCP relay proxy to receive requests from a DHCP client and send requests to the DHCP server, and then obtain DHCP information from the server and return it to the client.

To create a DHCP relay proxy, take the following steps:

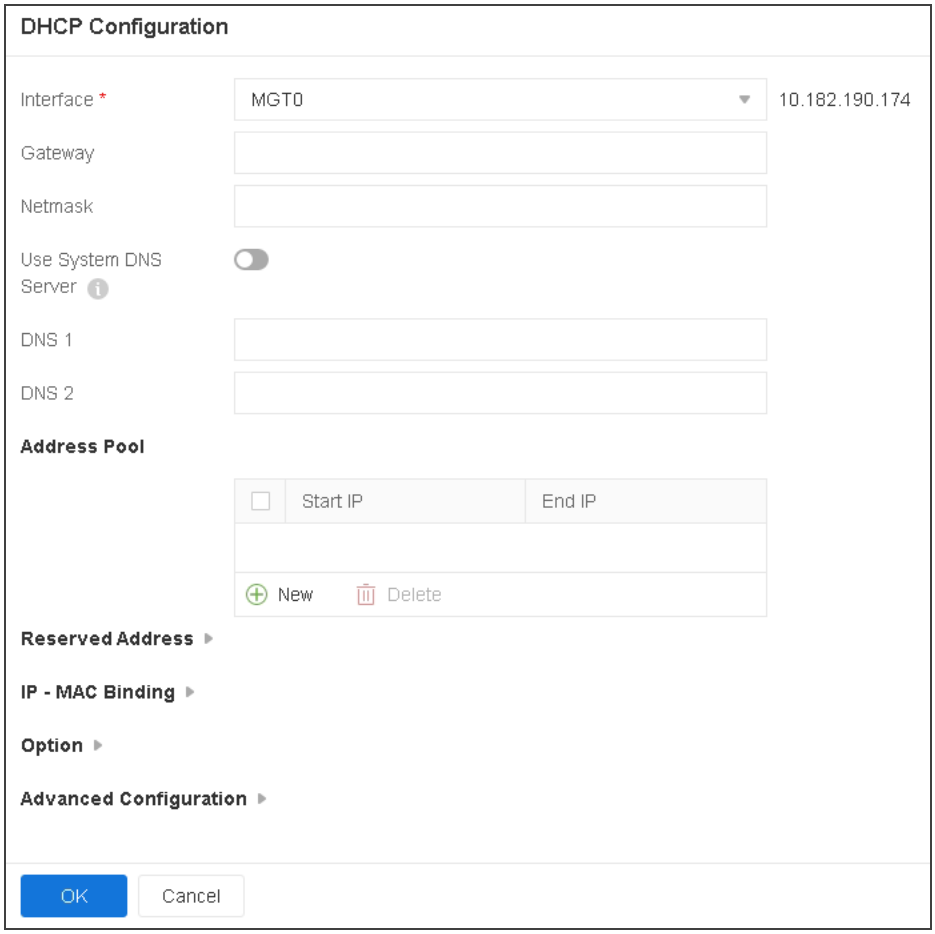
1. Select **Network > DHCP**.
2. Click **New > DHCP Relay Proxy**.
3. In the DHCP Relay Proxy page, select an interface to which the DHCP Relay Proxy will be applied from the Interface drop-down list.
4. Type the IP addresses of DHCP servers into the Server 1/Server 2/Server 3 boxes.
5. Click **OK**.

Notes: To ensure that clients can successfully obtain IP addresses, the administrator needs to configure DHCP relay permit policies in the direction from the DHCP server to clients.

Configuring a DHCPv6 Server

To create a DHCPv6 server to appropriate IPv6 addresses, take the following steps:

1. Select **Network > DHCP**.
2. Select **New > DHCPv6 Server**.



3. In the DHCPv6 Configuration page, configure as following:

Option	Description
Interface	Configures a interface which enables the DHCPv6 server to appropriate IPv6 addresses.
rapid-commit	Clicking this button can help fast get IPv6 address from the server. You need to enable both of the DHCP client and server's Rapid-commit function.
Preference	Specifies the priority of the DHCPv6 server. The range should be from 0 to 255. The bigger the value is, the higher the priority is.

Option	Description
Use System DNS Server	Click Enable. This way, the DNS server configured in the system is used as the DNS server of the client. Note: • If the system has configured more than two DNS servers, you can use the first two DNS servers as the DNS servers of the client; • After you enable Use System DNS Server, the system prioritizes providing DNS servers to the client by using this function.
DNS1	Configures a primary DNS server for the client. Type the server's IP address into the box.
DNS2	Configures an alternative DNS server for the client. Type the server's IP address into the box.
Domain	Configures the domain name for the DHCP client.
Address Pool: System can act as a DHCPv6 server to allocate IPv6 addresses for the DHCP clients in the subnets.	
IP	Specifies the IPv6 address prefix and prefix length.
Valid Lifetime	Specifies the lifetime of the address.
Preferred Lifetime	Specifies the preferred lifetime for the IPv6 address. The preferred lifetime should not be larger than the valid lifetime.

4. Click **OK**.

Configuring a DHCPv6 Relay Proxy

The device can act as a DHCPv6 relay proxy to receive requests from a DHCPv6 client and send requests to the DHCPv6 server, and then obtain DHCP information from the server and return it to the client.

To create a DHCPv6 relay proxy, take the following steps:

1. Select **Network > DHCP**.
2. Click **New > DHCPv6 Relay Proxy**.
3. In the DHCP Relay Proxy page, select an interface to which the DHCPv6 Relay Proxy will be applied from the Interface drop-down list.
4. Type the IPv6 addresses of DHCPv6 servers into the Server 1/Server 2/Server 3 boxes.
5. If the DHCPv6 server is specified as link-local address, you need to select the egress interface name from Egress Interface 1/Egress Interface 2/Egress Interface 3 dropdown list.
6. Click **OK**.

DDNS

DDNS (Dynamic Domain Name Server) is designed to resolve fixed domain names to dynamic IP addresses. Generally you will be allocated with a dynamic IP address from ISP each time you connect to the Internet, i.e., the allocated IP addresses for different Internet connections will vary. DDNS can bind the domain name to your dynamic IP address, and the binding between them will be updated automatically each time you connect to the Internet.

In order to enable DDNS, you will have to register in a DDNS provider to obtain a dynamic domain name. Hillstone devices support the following 5 DDNS providers, and you can visit one of the following websites to complete the registration:

- dyndns.org: http://dyndns.com/dns
- 3322.org: http://www.pubyun.com (This is unavailable for the v3 license)

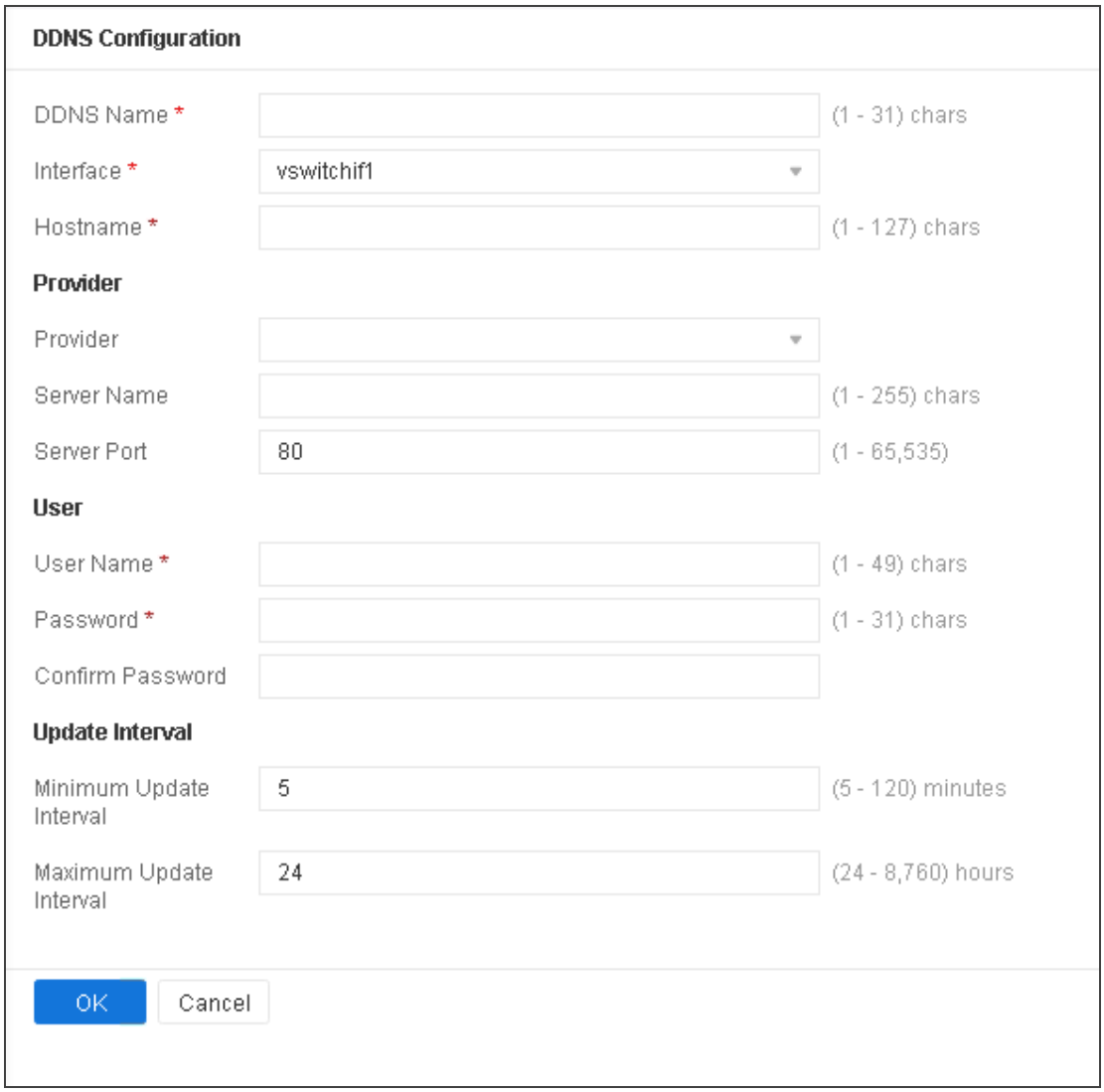
- no-ip.com: http://www.noip.com
- Huagai.net: http://www.ddns.com.cn (This is unavailable for the v3 license)
- ZoneEdit.com: http://www.zoneedit.com

Configuring a DDNS

To create a DDNS, take the following steps:

1. Select **Network > DDNS**.

2. Click **New**.



3. In the DDNS Configuration page, configure as follows:

Option	Description
DDNS Name	Specifies the name of DDNS.
Interface	Specifies the interface to which DDNS is applied.

Option	Description
Hostname	Specifies the domain name obtained from the DDNS provider.
Provider	
Provider	Specifies a DDNS provider. Choose one from the drop-down list.
Server Name	Specifies a server name for the configured DDNS.
Server Port	Specifies a server port number for the configured DDNS. The value range is 1 to 65535.
User	
User Name	Specifies the user name registered in the DDNS provider.
Password	Specifies the corresponding password.
Confirm Password	Enter the password again to confirm.
Update Interval	
Minimum Update Interval	When the IP address of the interface with DDNS enabled changes, system will send an update request to the DDNS server. If the server does not respond to the request, system will send the request again according to the configured min update interval. For example, if the minimum update interval is set to 5 minutes, then system will send the second request 5 minutes after the first request failure; if it fails again, system will send the third request 10 (5x2) minutes later; if it fails again, and system will send the forth request 20 (10*2) minutes later, and so forth. The value will not increase anymore when reaching 120

Option	Description
	minutes. That is, system will send the request at a fixed interval of 120 minutes. The default value is 5.
Maximum Update Interval	In case the IP address has not changed, system will send an update request to the DDNS server at the maximum update interval. Type the maximum update interval into the box. The value range is 24 to 8760 hours. The default value is 24.

4. Click **OK**.

Notes: The Server name and Server port in the configuration options must be the corresponding name and port of the DDNS server. Do not configure these options if the exact information is unknown. The server will return the name and port information automatically after connection to the DDNS server has been established successfully.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, combines PPP protocol and Ethernet to implement access control, authentication, and accounting on clients during an IP address allocation.

The implementation of PPPoE protocol consists of two stages: discovery stage and PPP session stage.

- Discovery stage: The client discovers the access concentrator by identifying the Ethernet MAC address of the access concentrator and establishing a PPPoE session ID.
- PPP session stage: The client and the access concentrator negotiate over PPP. The negotiation procedure is the same with that of a standard PPP negotiation.

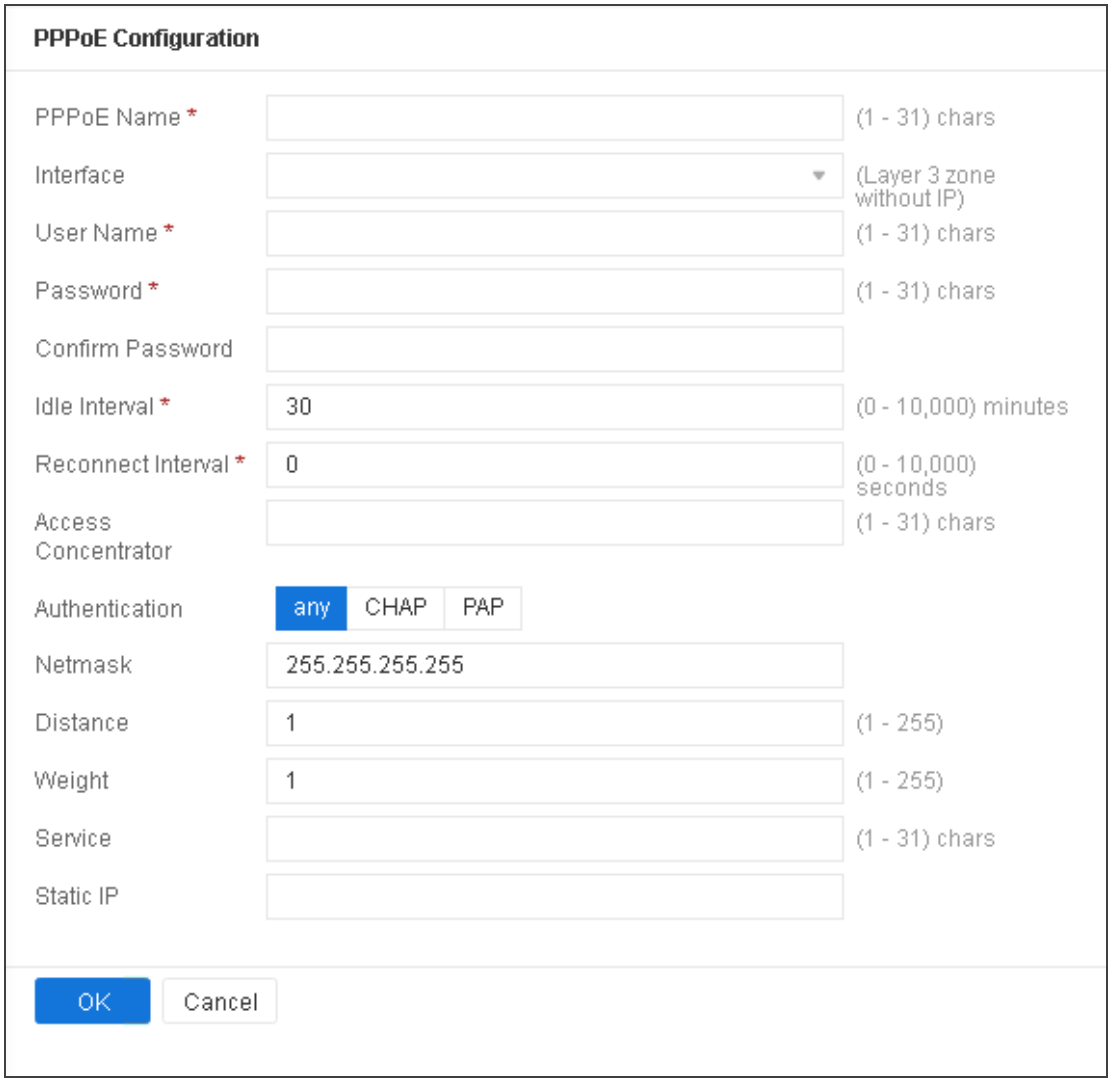
Interfaces can be configured as PPPoE clients to accept PPPoE connections.

Configuring PPPoE

To create a PPPoE instance, take the following steps:

1. Select **Network > PPPoE**.

2. Click **New**.



3. In the PPPoE Configuration page, configure as follows.

Option	Description
PPPoE Name	Specifies a name for the PPPoE instance.
Interface	Select an interface from the drop-down list.
User Name	Specifies a username.
Password	Specifies the corresponding password.
Conform Password	Enter the password again to confirm.
Idle Interval	Automatic connection. If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 0.
Reconnect Interval	If the PPPoE connection disconnects for any reason for a certain period, i.e. the specified re-connect interval, system will try to re-connect automatically. The value range is 0 to 10000 seconds. The default value is 10, which means the function is disabled.
Access Concentrator	Specifies a name for the concentrator.
Authentication	The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default,

Option	Description
	anyone between CHAP and PAP). To configure a PPPoE authentication method, click the authentication you want to select. The configured authentication must be the same with that configured in the PPPoE server.
Netmask	Specifies a netmask for the IP address obtained via PPPoE.
Distance	Specifies a route distance. The value range is 1 to 255. The default value is 1.
Weight	Specifies a route weight. The value range is 1 to 255. The default value is 1.
Service	Specifies allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, system will accept any service returned from the server automatically.
Static IP	You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the Static IP box.

4. Click **OK**.

Virtual Wire

The system supports the VSwitch-based Virtual Wire. With this function enabled and the Virtual Wire interface pair configured, the two Virtual Wire interfaces form a virtual wire that connects the two subnetworks attached to the Virtual Wire interface pair together. The two connected sub-networks can communicate directly on Layer 2, without other sub network's forwarding. Furthermore, controls of policy rules or other functions are still available when Virtual Wire is used.

Virtual Wire operates in two modes, which are Strict and Non-Strict mode respectively, as detailed below:

- **Strict Virtual Wire mode**: In this mode, Hillstone devices does not need to perform MAC address learning. Packets can only be transmitted between Virtual Wire interfaces, and the VSwitch cannot operate in Hybrid mode. Any PC connected to Virtual Wire can neither manage devices nor access Internet over this interface.
- **Non-Strict Virtual Wire mode**: In this mode, Hillstone devices can perform MAC address learning. Packets can be transmitted between Virtual Wire interfaces, and the VSwitch also supports data forwarding in Hybrid mode. That is, this mode only restricts Layer 2 packets' transmission between Virtual Wire interfaces, and does not affect Layer 3 packets' forwarding.

The table below lists packet transmission conditions in Strict Virtual Wire and Non-Strict Virtual Wire mode. You can choose an appropriate Virtual Wire mode according to the actual requirement.

Packet	Strict	Non-strict
Egress and ingress are interfaces of one Virtual Wire interface pair	Allow	Allow
Ingress is not Virtual Wire's interface	Deny	Deny
Egress and ingress are interfaces of different Virtual Wire interface pairs	Deny	Deny
Ingress of to-self packet is a Virtual Wire’ s interface	Deny	Allow
Ingress is Virtual Wire's interface, and egress is a Layer 3 interface	Deny	Allow

Configuring a Virtual-Wire

To create a Virtual-Wire, take the following steps:

1. Select **Network > Virtual-Wire**.
2. Click **New**.
3. In the Virtual-Wire Configuration page, select a virtual switch from the VSwitch drop-down list.
4. In the Interface 1 drop-down list, specify an interface for the virtual wire interface pair. The two interfaces in a single virtual wire interface pair must be different, and one interface cannot belong to two different virtual wire interface pairs simultaneously.
5. In the Interface 2 drop-down list, specify an interface for the virtual wire interface pair. The two interfaces in a single virtual wire interface pair must be different, and one interface cannot belong to two different virtual wire interface pairs simultaneously.
6. Click **OK**.

Configuring the Virtual Wire Mode

To configure a virtual wire mode, take the following steps:

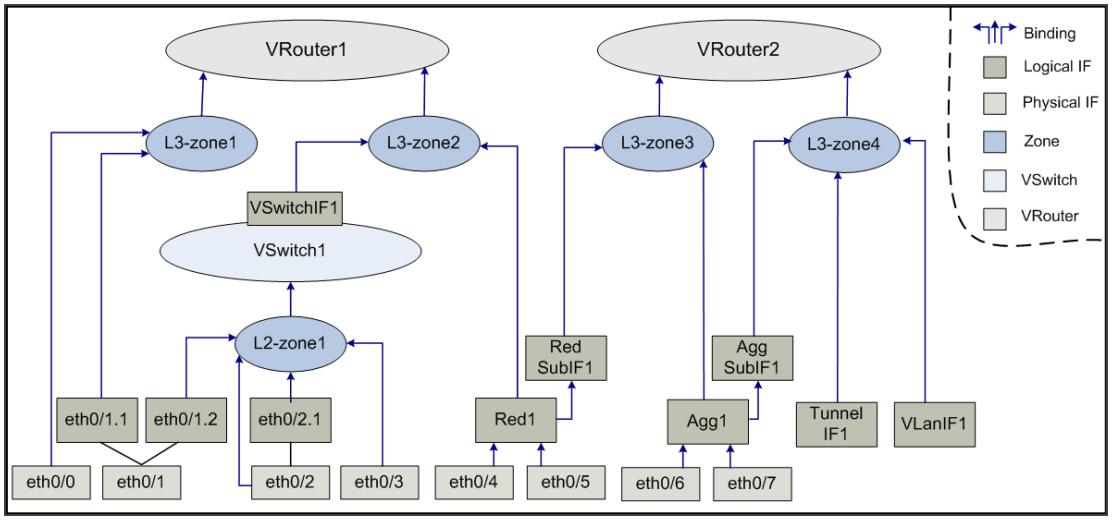
1. Select **Network > Virtual-Wire**.
2. Click **Virtual-Wire Mode**.
3. In the Virtual-Wire Mode Configuration page, select a virtual switch from the VSwitch drop-down list.
4. Specify a virtual wire mode from one of the following options:
    - Strict - Packets can only be transmitted between virtual wire interfaces, and the VSwitch cannot operate in Hybrid mode. Any PC connected to the virtual wire can neither manage devices nor access Internet over this interface.

- Non-strict - Packets can be transmitted between virtual wire interfaces, and the VSwitch also supports data forwarding in Hybrid mode. That is, this mode only restricts Layer 2 packets' transmission between virtual wire interfaces, and does not affect Layer 3 packets' forwarding.
- Disabled - Disables the virtual wire.

5. Click **OK**.

Virtual Router

Virtual Router (VRouter) is known as VR in system. VR acts as a router, and different VRs have their own independent routing tables. A VR named "trust-vr" is implemented with the system, and by default, all of the Layer 3 security zones are bounded to the trust-vr automatically. Hillstone devices support multiple VRs, and the max amount of supported VRs may vary with different hardware platforms. Multiple VRs divide a device into multiple virtual routers, and each router utilizes and maintains their independent routing table. In such a case one device is acting as multiple routers. Multiple VRs allow a device to achieve the effects of the address isolation between different route zones and address overlapping between different VRs, as well as to avoid route leaking to some extent, enhancing route security of network. For more information about the relationship between interface, security zone, VSwitch and VRouter, see the following diagram:



As shown above, the binding relationship between them are:

- Interfaces are bound to security zones. Those that are bound to Layer 2 security zones and Layer 3 security zones are known as Layer 2 interfaces and Layer 3 interfaces respectively. One interface can be only bound to one security zone; the primary interface and sub interface can belong to different security zones.
- Security zones are bound to a VSwitch or VRouter. Layer 2 security zones are bound to a VSwitch (by default the pre-defined Layer 2 security zone is bound to the default VSwitch1), and Layer 3 security zones are bound to a VRouter (by default the pre-defined Layer 3 security zone is bound to the default trust-vr), thus realizing the binding between the interfaces and VSwitch or VR. One security zone can be only bound to one VSwtich or VR.

Creating a Virtual Router

To create a Virtual Router, take the following steps:

1. Select **Network > Virtual Router > Virtual Router**.
2. Click **New**.
3. Type the name into the Virtual Router name box.
4. Click **OK**.

Global Configuration

Virtual Router's global configuration is the configuration for multiple Virtual Routers. To configure Multi-Virtual Router, take the following steps:

1. Select **Network > Virtual Router > Global Configuration**.
2. Click the **Enable** button for Multi-Virtual Router.
3. Click **Apply**.

Notes:

- After Multi-Virtual Router is enabled or disabled, system must reboot to make it take effect. After rebooting, system's max concurrent sessions might decrease if the function is enabled, or restore to normal if the function is disabled. For more information about the maximum concurrent sessions, see "The Maximum Concurrent Sessions" on Page 1847.
- If Multi-Virtual Router is enabled, traffic can traverse up to 3 Virtual Routers, and any traffic that has to traverse more than 3 Virtual Routers will be dropped.

Virtual Switch

System might allow packets between some interfaces to be forwarded in Layer 2 (known as transparent mode), and packets between some interfaces to be forwarded in Layer 3 (known as routing mode), specifically depending on the actual requirement. To facilitate a flexible configuration of hybrid mode of Layer 2 and Layer3, system introduces the concept of Virtual Switch (VSwitch). By default system uses a VSwitch known as VSwitch1. Each time you create a VSwitch, system will create a corresponding VSwitch interface (VSwitchIF) for the VSwitch automatically. You can bind an interface to a VSwitch by binding that interface to a security zone, and then binding the security zone to the VSwitch.

A VSwitch acts as a Layer 2 forwarding zone, and each VSwitch has its own independent MAC address table, so the packets of different interfaces in one VSwitch will be forwarded according to Layer 2 forwarding rules. You can configure policy rules conveniently in a VSwitch. A VSwitchIF virtually acts as a switch uplink interface, allowing packets forwarding between Layer 2 and Layer 3.

Creating a VSwitch

To create a VSwitch, take the following steps:

1. Select **Network > VSwitch**.

2. Click **New**.

Option	Description
VSwitch Name	Specifies a name for the VSwitch.
Virtual-Wire Mode	Specifies a Virtual-Wire mode for the VSwitch, including (for specific information on Virtual Wire, see "Virtual Wire" on Page 291) • Strict - Packets can only be transmitted between Virtual Wire interfaces, and the VSwitch cannot operate in Hybrid mode. Any PC connected to Virtual Wire can neither manage devices nor access Internet over this interface. • Non-strict - Packets can be transmitted between Virtual Wire interfaces, and the VSwitch also supports data forwarding in Hybrid mode. That is, this mode only restricts Layer 2 packets' transmission between Virtual Wire interfaces, and does not affect Layer 3 packets' forwarding. • Disabled - Disables Virtual Wire.
IGMP Snooping	Enables IGMP snooping on the VSwitch.
Forward Tagged Packets	Enables VLAN transparent so that the device can transmit VLAN tagged packets transparently, i.e., packets tagged with VLAN ID will still keep the original ID after passing through

Option	Description
	the device.
Forward Double Tagged Packets	Enables VLAN transparent so that the device can transmit VLAN double tagged packets transparently, i.e., packets tagged with VLAN ID will still keep the original ID after passing through the device.
Drop Unknown Multicast Packets	Drops the packets sent to unknown multicast to save bandwidth.

3. Click **OK**.

Port Mirroring

The device is designed with port mirroring on Ethernet interfaces. The port mirroring function forwards mirrored traffic based on the switch chip. Interfaces within the same switch chip belong to the same mirroring group. In this group, you can forward traffic from one or more source interfaces to another interface, enabling a traffic analysis device to monitor and analyze the traffic. This facilitates rapid fault location when a network issue occurs. The one or more source interfaces are called the "source interface of port mirroring", and the other interface is called the "destination interface of port mirroring".

Limits and Precautions

- The source and destination interfaces needs to be Ethernet interfaces. To serve as a destination interface, an Ethernet interface cannot not be bound to a security zone.

- Traffic mirroring can only occur between interfaces within the same mirroring group: the source and destination interfaces need to belong to the same group. Cross-group mirroring is not supported.
- Only one destination interface is allowed, but there is no limit on the number of source interfaces.
- An interface cannot simultaneously serve as both a source and a destination interface.
- The destination interface needs to be directly connected to the packet analysis device.
- MGT and HA interfaces do not support the port mirroring function.
- Port mirroring does not support IPv6.
- Enabling the port mirroring function will consume the bandwidth resources of the device, degrading the performance of the device in handling traffic. It is recommended to disable the function promptly after use.

Destination interface of port mirroring supported on Ethernet interfaces:

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules
SG-6000-A7600/A6800	No	No
SG-6000-A5800/A5600/A5555/A5255/A5155	Yes (E0/0-E0/7 and XE0/8-XE0/9	No

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules	
	belong to the same mirroring group; XE0/10-XE0/23 and XLE0/24-XLE0/25 belong to the same mirroring group)		
SG-6000-A5500/A5200/A5100	Yes (except XE0/26-XE0/29)	No	
SG-6000-A3815/A3615/A2815/A2715	Yes	IOC-A-F-4SFP+ IOC-A-F-8SFP+	Yes (Ethernet interfaces on the expansion module and on the front panel belong to two different mirroring groups.)
		IOC-A-F-8GE	Yes (Ethernet interfaces on the expansion module

Model	Destination Interface of Port Mirroring Supported on Ethernet interfaces on the Front Panel	Destination Interface of Port Mirroring Supported on Ethernet interfaces on Expansion Modules
		and on the front panel belong to the same mirroring groups.)
SG-6000-A3800/A3700	Yes	No
SG-6000-A3600/A3000/A2800/A2700/A2600/A2000/A1100/A200	Yes	Expansion module is not supported.
A1000	Yes	Expansion module is not supported.



Notes:

- Port mirroring is only supported on Ethernet interfaces that are in the same mirroring group. Port mirroring across mirroring groups is not supported.
- Port mirroring is not supported on the MGT interface and HA interface.

To configure port mirroring, take the following steps:

1. Enable port mirroring on an Ethernet interface, and select the traffic type to be mirrored.
2. Configure a destination interface.

To configure the destination interface of port mirroring:

1. Select **Network > Port Mirroring**.
2. Select an interface from the Destination Interface drop-down list, and click **OK**. All the source and destination interface will be listed in the table below.

WLAN

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

WLAN (Wireless Local Area Network) represents the local area network that uses the wireless channel as the medial. WLAN is important supplements and extensions of the wired LAN. By configuring the WLAN function, you can establish the wireless local area network and allow the users to access LAN through wireless mode.

Creating a WLAN

Notes: The system of A200W allows you to create at most 2 WLAN. You can connect to any one of them to access the LAN.

To create a WLAN, take the following steps:

1. Select **Network > WLAN**.
2. Click **New**.

Option	Description
SSID	Specifies the name of the WLAN.
WLAN Interface	Specifies the WLAN interface bound to this newly-created WLAN.
SSID Broadcast	Click the **Enable** button to enable the SSID broadcast. After enabling SSID broadcast, any user can search it.
Security Mode	Configures the security mode:

Option	Description
	• No encryption - Do not perform the encryption. • MAC-PSK - Integrates MAC authentication with WPA-WPA2-PSK authentication. • WEP - Specifies the security mode as wired equivalent privacy. • WPA、WPA2 - Specifies the security mode as Wi-FI and uses 802.1X authentication. WPA and WPA2 have stronger performance than WEP. The safety of WPA2 is more reliable than WPA. • WPA-WPA2 - Compatible with WPA and WPA-2. • WPA-PSK、WPA2-PSK - Specifies the security mode as Wi-FI and uses the pre-shared key authentication. • WPA-WPA2-PSK - Compatible with WPA-PSK and WPA2-PSK.
Link-layerAuthentication Mode	When using the WEP security mode, specify the authentication mode for the WLAN. • open-system - The default authentication mode. This is the easiest authentication, ie. do not need to certify. • shared-key - Certify with the same shared key authentication.

Option	Description
Data Encryption	When using a security mode besides WEP, specifies the data encryption mode, including TKIP, CCMP, and TKIP-CCMP.
Key	When using the WEP security mode, specify the form and the value of the key. The form of the key can be a character string or a hexadecimal number. When using character strings, you can specify 5 characters or 13 characters. When using hexadecimal numbers, you can specify 10 hexadecimal numbers or 26 hexadecimal numbers.
Pre-shared Key	When using the MAC-PSK, WPA-PSK, WPA2-PSK, WPA-WPA2-PSK security modes, specify the form and the value of the pre-defined key. The form of the key can be a character string or a hexadecimal number. When using character strings, you can specify 8-63 characters. When using hexadecimal numbers, you can specify 64 hexadecimal numbers.
Maximum Users	Specifies the allowed maximum number of users that can access this WLAN. The value ranges from 1 to 128. The default value is 64.
User Isolation	Select **Enable** to enable the user isolation function. After enabling the user isolation, users within one WLAN cannot access each other. User isolation enhances the security for different users.
AAA Server	When specifying the security mode as WPA, WPA2, WPA-WPA2, or MAC-PSK, you must select a configured

Option	Description
	AAA server as the authentication server for user identification.

3. Click **OK**.

Advanced Settings

To configure the advanced settings for WLAN, take the following steps:

1. Select **Network > WLAN**.
2. Click **Advanced**.

3. In the Advanced page, configure the following information.

Option	Description
Countries & Regions	Different countries or regions have different management and limitations on RF use. The country/region code determines the available frequency range, channel, and legal level of transmit power. The default value is United States.
Working Mode	Configure the working mode. • 802.11a represents that the interface works in the 802.11a mode. • 802.11b represents that the interface works in the 802.11b mode. • 802.11g represents that the interface works in the 802.11g mode. • 802.11an represents that the interface works in the 802.11n mode of 5GHz. • 802.11bgn represents that the interface works in the 802.11n mode of 2.4GHz.
Channel	The available channels you can select vary with the country/region code and RF type. The default value is auto, which represents to ask the system to select the channel automatically. After the country/region code or the operation mode is changed, system will select the channel automatically.
Maximum Trans-	The maximum transmit power varies with the country/region

Option	Description
mit Power	code and RF type. By default, there are four levels: 12.5% of the maximum transmit power, 25% of the maximum transmit power, 50% of the maximum transmit power, and 100% of the maximum transmit power.

4. Click **OK**.

3G/4G

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The third generation of mobile telecommunications technology supports the high speed data transmission. By configuring the 3G/4G function, users can access the Internet through wireless mode.

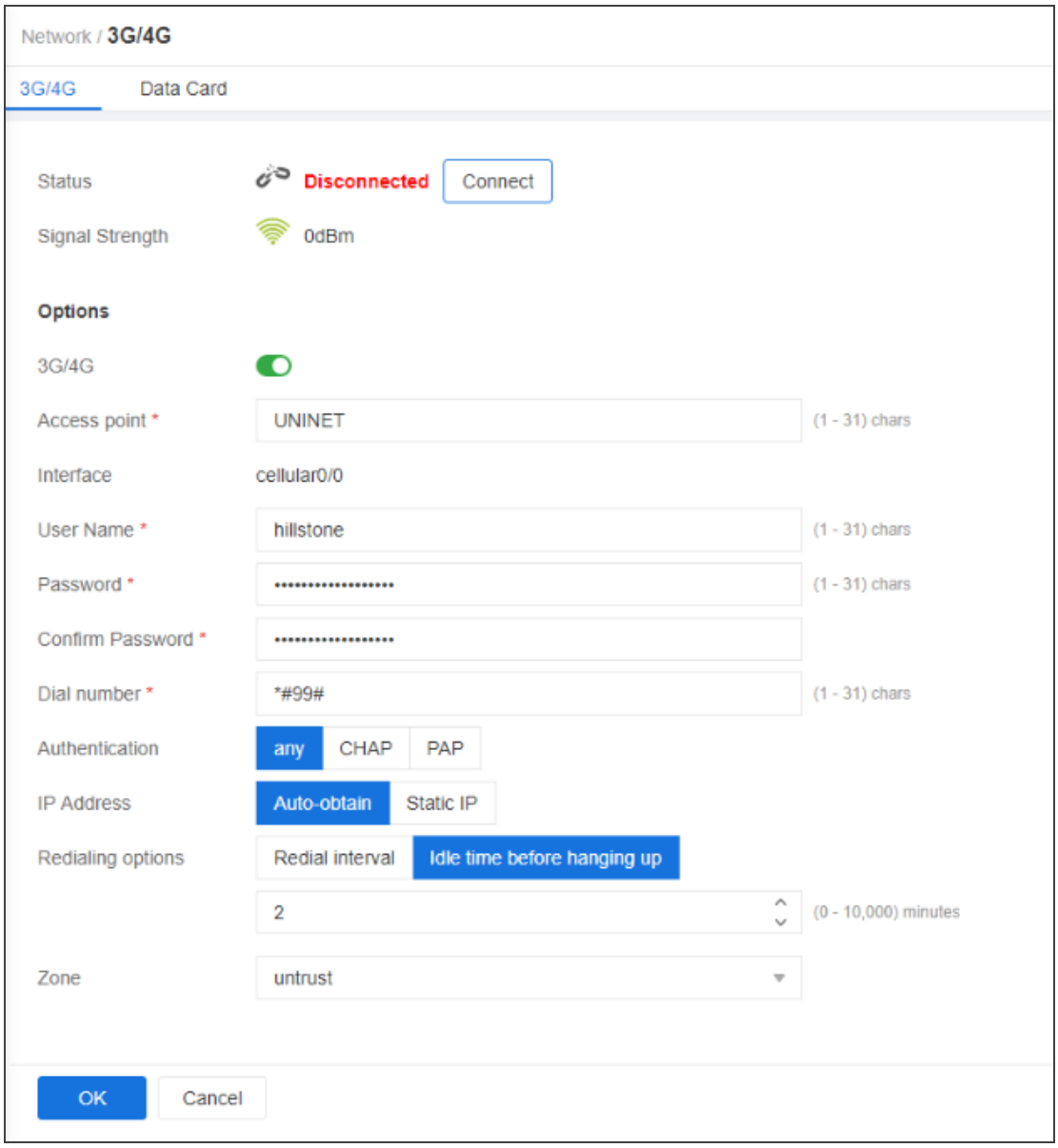
The 3G/4G function needs the support of ISP. Before configuring the 3G/4G function, you need to purchase the SIM card from the ISP, enable the data connection service, and obtain the following 3G/4G parameters: access point, username, password, dial-up string, and correctly installed SIM card.

Some A-series devices can access the Internet by external 4G modules of ZTE MF79U and MF833V being inserted into the USB port. Platforms that support external 4G modules are SG-6000-A200/A200W. The SIM card of the external 4G module is not hot swappable.

Configuring 3G/4G Settings

To configure 3G/4G settings, take the following steps:

1. Select **Network > 3G/4G**.



2. In the 3G/4G tab, you can view the 3G/4G connection status in the Status section. Click **Connect** to connect to the 3G network.

3. Select **Enable** to enable the 3G/4G function. By default, the 3G function is enabled.

4. Enter the name of the access point in the Access point text box. You can enter up to 31 characters.

5. Specify the 3G/4G user information. In the User Name text box, enter the username of the 3G/4G user. You can enter up to 31 characters. In the Password text box, enter the corresponding password.

6. Configure the dial-up string. Ask your ISP to provide the dial-up string and enter the dial-up string in the Dial number text box.

7. Specify the authentication mode. When 3G/4G dial-up establishes the connection, it needs to pass the PPP protocol verification. The device supports the following verification methods: CHAP, PAP, and Any. Select the desired method by selecting the Authentication radio button.

8. Configure the IP address information for the 3G/4G interface. Select **Auto-obtain** to make the 3G/4G interface obtain the IP address automatically. Select **Static IP** to enter the static IP address and the netmask.

9. Specify the online mode in Redialing options. 3G/4G dial-up has two online modes as follows:

    - Redial interval: When the 3G/4G connection disconnects due to certain reasons and the disconnection time exceeds the specified time interval, system will redial automatically. Specify the time interval in the Redial interval text box. The value ranges from 0 to 10000 seconds. The default value is 0, which represents that the system does not use the **redial automatically** mode.

    - Idle time before hanging up: When the idle time of the 3G/4G (cellular) interface reaches the specified value, system will disconnect the 3G/4G connection. Specify the length of time in the Idle time before hanging up text box. The value ranges from

0 to 10000 seconds. The default value is 0, which represents that the system does not use the **hang up after a specified idle time** mode

> **Notes:** The above two modes cannot be used simultaneously. Without configuring the schedule, system will use the "Redial interval" mode by default.

10. Specify the security zone of the 3G/4G interface.
11. Click **OK**.

> **Notes:** After installing the SIM card, system can automatically configure the settings in the 3G/4G tab based on the information of the 3G/4G module. The settings include the name of the access point, 3G/4G user information, and dial-up string. You can modify the settings according to your requirements.

Managing Data Card

PIN (Personal Identification Number) code is used to identify the user of the SIM card and avoid the illegal use of the SIM card. If you have high security requirements for the 3G/4G network, you can enable the PIN protection function on the data card management configuration page to better protect the network. With the PIN code protection enabled, SIM card can be used only after the PIN code is verified. If the device uses external 4G module of ZTE MF79U to access the Internet, the 4G module can be identified and used only after password authentication.

4G Module Password Authentication

To authenticate the 4G module with password, take the following steps:

1. Select **Network > 3G/4G**.
2. Click **Data Card** tab.

3. In the **4G Module Password Authentication** section, enter the verification password in the **Password** text box. The value ranges from 1 to 31 characters.
4. Click **Apply**.

Automatically Verifying the PIN Code

After enabling the PIN code protection, you can save the PIN code in system. After system reboots, it can automatically verify the PIN code.

To automatically verify the PIN code, take the following steps:

1. Select **Network > 3G/4G**.
2. Click **Data Card** tab.
3. Enter the PIN code in the PIN Code text box. The value ranges from 4 to 8 numbers.
4. Click **Apply** to make the system save the PIN code.

Notes: After three consecutive failed attempts at PIN code, the SIM card will be locked.

Enabling/Disabling the PIN Code Protection

To enable/disable the PIN code protection, take the following steps:

1. Select **Network > 3G/4G**.
2. Click **Data Card** tab.
3. Click Enable PIN code protection in the PIN code management section to enable the PIN code protection function. To disable the function, click Disable PIN code protection.

4. Enter the PIN code in the PIN code text box. The PIN code consists of 4-8 decimal numbers.
5. Click **Apply**.

Modifying the PIN Code

To modify the PIN code, take the following steps:

1. Select **Network > 3G/4G**.
2. Click **Data Card** tab.
3. Click Change PIN code in the PIN code management section.
4. Specify the current PIN code in the Current PIN code text box. The PIN code consists of 4-8 decimal numbers.
5. Specify a new PIN code in the New PIN code text box. The PIN code consists of 4-8 decimal numbers.
6. Confirm the new PIN code in the Confirm PIN code text box.
7. Click **Apply**.

Manually Verifying the PIN Code

To manually verify the PIN code, take the following steps:

1. Select **Network > 3G/4G**.
2. Click **Data Card** tab.
3. Click Verify PIN Code in the PIN code management section.
4. Enter the PIN code in the PIN code text box. The PIN code consists of 4-8 decimal num-

bers.

5. Click **Apply**.

Unlocking the PIN Code

If the SIM card is locked, you need to obtain the PUK code from the ISP to unlock the SIM card and set the new PIN code. To use the PUK code to unlock the PIN code, take the following steps:

1. Select **Network > 3G/4G**.
2. Click **Data Card** tab.
3. Click **Unlock PIN Code** in the PIN code management section.
4. Enter the PUK code in the PUK code text box.
5. Specify a new PIN code in the New PIN code text box. The PIN code consists of 4-8 decimal numbers.
6. Confirm the new PIN code in the Confirm PIN code text box.
7. Click **Apply**.

Load Balancing

SLB

The Server Load Balancing (SLB) function can distribute traffic to different intranet servers by using load balancing algorithms, fully utilizing each intranet server and improving business processing capacities. The SLB function can be implemented by using one of the following methods:

- Balancing traffic to the specified port on different intranet servers: This is suitable for scenarios where different intranet servers provide the same application service on their respective

specified port simultaneously.

- Balancing traffic to different ports on the same intranet server: This is suitable for scenarios where the same server runs multiple processes on different ports to provide the same application service.
- Combining the two methods above for traffic balancing.



Notes: The SLB function can be configured only by using the CLI. For more information, refer to *StoneOS CLI User Guide*.

LLB

For multiple ISP links, the system uses real-time link monitoring technology and dynamic link detection technology to distribute traffic reasonably across different links, reducing network latency, jitter, and packet loss rate on each link, achieving a more balanced bandwidth utilization. You can enable LLB respectively for outbound and inbound traffic. Two different dynamic link detection technologies are used for outbound and inbound traffic, namely real-time link monitoring technology for outbound traffic and SmartDNS technology for inbound traffic. Based on the detection results, automatic load balancing of traffic is achieved.

This topic consists of the following sections:

- "Inbound Link Load Balancing" on Page 337
- "Outbound Link Load Balancing" on Page 315

Outbound Link Load Balancing

In the outbound direction, the system implements intelligent routing based on real-time monitoring of the latency, jitter, packet loss rate, and bandwidth utilization of each link, and dynamically adjusts the traffic load on each link. You can configure flexibleSLA profiles and LLB Profiles and bind them with routing (the system only supports destination-based routes and policy-based routes) to form LLB rules, which can control and load balance outbound link traffic.

Outbound Load Balancing Implementation Mechanism

Outbound load balancing implementation mechanism is as follows:

1. Based on business requirements, users customize the SLA link quality measurement criteria. The system will dynamically detect the quality of outbound links in real time, including latency, jitter, and packet loss rate, and compare them with the thresholds set in the profile to filter available outbound links.
2. The LLB further optimizes the selected available outbound links (Links that meet the SLA measurement criteria) by comprehensively calculating the cost of each link based on key parameters such as latency weight, packet loss weight, jitter weight, and bandwidth weight.
3. The system allocates more outbound traffic to links with lower costs while reducing traffic allocation on links with higher costs, achieving efficient and balanced outbound traffic load.
4. If none of the links meet the SLA measurement criteria, the LLB will forward traffic based on the cost of all links.

Configuration Method

Please follow the steps below to configure outbound load balancing:

- Configure an LLB profile

  The LLB profile contains parameters for load balancing algorithms, allowing you to flexibly

configure settings such as balancing mode, bandwidth utilization threshold, detection switch, detection mode, balancing direction, and the impact factor of link Cost value. The system will select links and balance traffic based on the configured parameters:

- If the balancing mode is the compatibility mode, the system will select the original link (cached link) for traffic forwarding. This mode is suitable for businesses sensitive to link switching, such as banking services.
- If network detection is enabled, the system will detect the network link status based on configured parameters to select the optimal link:
    - When the link's bandwidth utilization is below the specified threshold, the system calculates link quality based on latency weight, packet loss weight, and jitter weight, prioritizing links with a higher quality.
    - When the link's bandwidth utilization exceeds the specified threshold, the system calculates link quality based on latency weight, packet loss weight, jitter weight, bandwidth weight, link bandwidth, and bandwidth utilization, prioritizing links with a higher quality.
- If network detection is enabled and LLB rules are bound to a domain name book, the system will use real-time detection technology for domain names to ensure more accurate route selection. This method is suitable for link selection within specific domain name:
    - When the link's bandwidth utilization is lower than the specified threshold, the system calculates link quality based on latency weight, prioritizing links with a higher quality.

- When the link's bandwidth utilization exceeds the user-defined threshold, the system calculates link quality based on latency weight, bandwidth weight, link bandwidth, and bandwidth utilization, prioritizing links with a higher quality.



Notes: By default, network detection is enabled. You can use the **show llb profile** command to view the status of network detection. If the function is disabled, it can be enabled by using the **detect enable** command.

- Configure an LLB rule

  By configuring LLB rules, LLB profiles are bound to routes (the system only supports destination-based routes and policy-based routes) to control and load balance outbound link traffic.

If you need to filter the outbound links for traffic based on customized link quality criteria (such as latency, jitter, and packet loss rate), you can configure an SLA Profile. By using the SLA Profile to filter out links that meet the SLA standards, and binding the SLA Profile together with the LLB Profile to the route, you can achieve more precise control and balancing of link traffic.

Configuring Outbound Link Load Balancing

Before you start

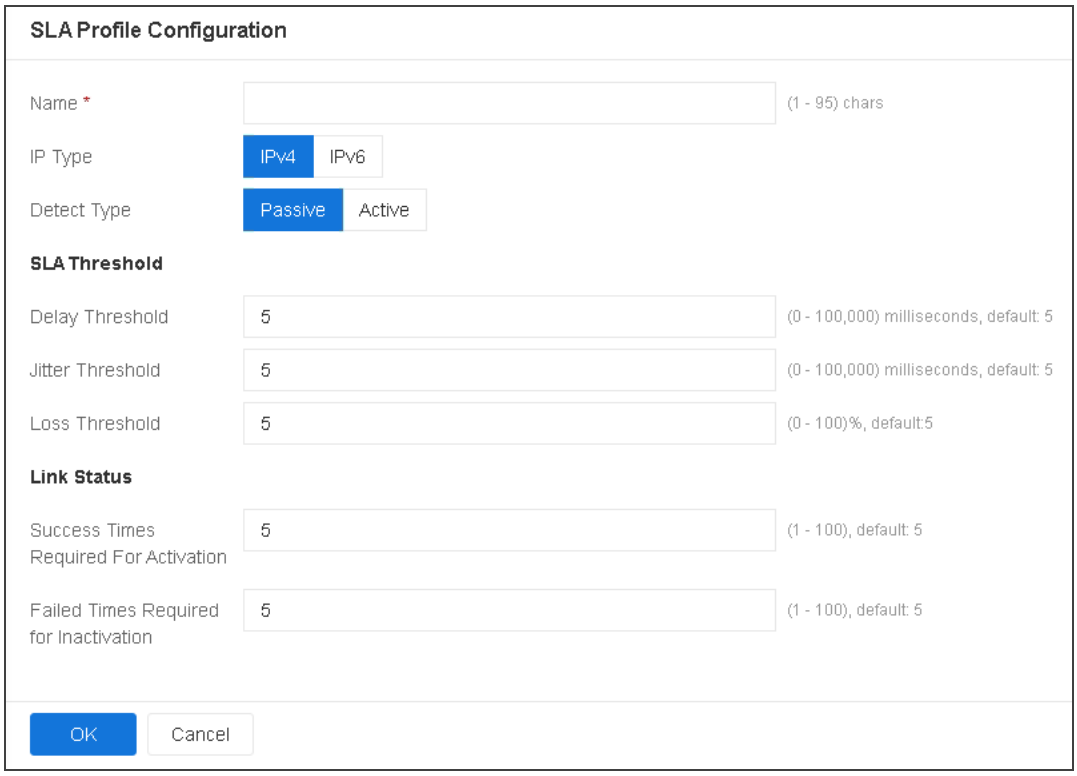
- **Read** "Outbound Link Load Balancing" on Page 315

Configuring SLA Profile

To configure an SLA profile, take the following steps:

1. Select **Network** > **Outbound LLB** > **SLA Profile**.

2. In the upper-left corner, click **New**.



Option	Description
Name	Specifies the name of the SLA Profile, which needs to be 1 to 95 characters in length.
IP Type	Specifies the IP type of the SLA Profile as IPv4 or IPv6. The default type is IPv4.
Detect Type	Specifies the detection type, including passive detection mode and active detection mode: • Passive - The passive detection mode samples TCP traffic on outbound links to obtain quality parameters such as latency, jitter, and packet loss rate of the links. This mode

Option	Description
	is the default mode. • Active - In active detection mode, the outbound interface of the link actively sends detection packets to specified destination addresses to obtain quality parameters such as latency, jitter, and packet loss rate of the links. When you select this mode, you need to specify the protocol type, destination address, detection interval, and number of sent packets for detection packets in subsequent configuration items.
Protocol	Specifies the protocol type for sending detection packets in active detection mode, which can be ICMP (ICMPV6) or TCP, with ICMP (ICMPV6) being the default. When you select TCP, you need to enter a TCP port number.
Address Type	Specifies the destination address for detection packets in active detection mode, which can be an IP address or a domain name. Once specified, you need to enter an IPv4 (IPv6) address or domain name in the corresponding field.
Detect Interval	Specifies the interval of sending detection packets in active detection mode. Valid values: 2 to 5 seconds. Default value: 2 seconds.
Packages Number	Specifies the number of detection packets to be sent in a single transmission in active detection mode. Valid values: 5 to 10. Default value: 5.

Option	Description
SLA Threshold	
Delay Threshold	Specifies the SLA delay threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no delay detection of link is performed.
Jitter Threshold	Specifies the SLA jitter threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no jitter detection of link is performed.
Loss Threshold	Specifies the SLA packet loss rate threshold. Valid values: 0 to 100 (0%-100%). Default value: 5. 0 indicates that no packet loss rate detection of link is performed.
Link Status	
Success Times Required For Activation	Specifies the number of successful activations required for a link to transition from inactive to active status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics falls below the configured threshold, the number of successful activations for the link increases by 1. When the cumulative activation count exceeds or equals the specified number of successful activations, the link transitions from inactive to active status, becoming an available outbound link. Valid values: 1 to 100. Default value: 5.
Failed Times Required For Inactivation	Specifies the number of failed deactivations required for a link to transition from active to inactive status. The system compares the detected link latency, jitter, and packet loss rate with the

Option	Description
	configured SLA thresholds. When any of these metrics exceeds the configured threshold, the number of failed deactivations for the link increases by 1. When the cumulative deactivation failure count exceeds or equals the specified number of failed deactivations, the link transitions from active to inactive status, becoming an unavailable outbound link. Valid values: 1 to 100. Default value: 5.

3. Click **OK**.
4. On the **SLA Profile** page, you can also perform the following operations:
   - Disable SLA profile: By default, a configured SLA profile is enabled. You can select one or more SLA profiles as required and click **Disable**. This way, these SLA profiles cannot be used for link quality detection and outbound path selection.
   - Enabling SLA profile: Select one or more SLA profiles as required and click **Enable** to enable them.
   - Edit SLA profile: Select an SLA profile and click **Edit** to edit the profile.
   - Delete SLA profile: Select one or more SLA profiles and click **Delete** to delete them.
5. Select **Network** > **Outbound LLB** > **SLA Profile**.

6. In the upper-left corner, click **New**.



Option	Description
Name	Specifies the name of the SLA Profile, which needs to be 1 to 95 characters in length.
IP Type	Specifies the IP type of the SLA Profile as IPv4 or IPv6. The default type is IPv4.
Detect Type	Specifies the detection type, including passive detection mode and active detection mode: • Passive - The passive detection mode samples TCP traffic on outbound links to obtain quality parameters such as latency, jitter, and packet loss rate of the links. This mode is the default mode.

Option	Description
	• Active - In active detection mode, the outbound interface of the link actively sends detection packets to specified destination addresses to obtain quality parameters such as latency, jitter, and packet loss rate of the links. When you select this mode, you need to specify the protocol type, destination address, detection interval, and number of sent packets for detection packets in subsequent configuration items.
Protocol	Specifies the protocol type for sending detection packets in active detection mode, which can be ICMP (ICMPV6) or TCP, with ICMP (ICMPV6) being the default. When you select TCP, you need to enter a TCP port number.
Address Type	Specifies the destination address for detection packets in active detection mode, which can be an IP address or a domain name. Once specified, you need to enter an IPv4 (IPv6) address or domain name in the corresponding field.
Detect Interval	Specifies the interval of sending detection packets in active detection mode. Valid values: 2 to 5 seconds. Default value: 2 seconds.
Packages Number	Specifies the number of detection packets to be sent in a single transmission in active detection mode. Valid values: 5 to 10. Default value: 5.
SLA Threshold	

Option	Description
Delay Threshold	Specifies the SLA delay threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no delay detection of link is performed.
Jitter Threshold	Specifies the SLA jitter threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no jitter detection of link is performed.
Loss Threshold	Specifies the SLA packet loss rate threshold. Valid values: 0 to 100 (0%-100%). Default value: 5. 0 indicates that no packet loss rate detection of link is performed.
Link Status	
Success Times Required For Activation	Specifies the number of successful activations required for a link to transition from inactive to active status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics falls below the configured threshold, the number of successful activations for the link increases by 1. When the cumulative activation count exceeds or equals the specified number of successful activations, the link transitions from inactive to active status, becoming an available outbound link. Valid values: 1 to 100. Default value: 5.
Failed Times Required For Inactivation	Specifies the number of failed deactivations required for a link to transition from active to inactive status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics exceeds

Option	Description
	the configured threshold, the number of failed deactivations for the link increases by 1. When the cumulative deactivation failure count exceeds or equals the specified number of failed deactivations, the link transitions from active to inactive status, becoming an unavailable outbound link. Valid values: 1 to 100. Default value: 5.

7. Click **OK**.
8. On the **SLA Profile** page, you can also perform the following operations:
   - Disable SLA profile: By default, a configured SLA profile is enabled. You can select one or more SLA profiles as required and click **Disable**. This way, these SLA profiles cannot be used for link quality detection and outbound path selection.
   - Enabling SLA profile: Select one or more SLA profiles as required and click **Enable** to enable them.
   - Edit SLA profile: Select an SLA profile and click **Edit** to edit the profile.
   - Delete SLA profile: Select one or more SLA profiles and click **Delete** to delete them.
9. Select **Network** > **Outbound LLB** > **SLA Profile**.

10. In the upper-left corner, click **New**.



Option	Description
Name	Specifies the name of the SLA Profile, which needs to be 1 to 95 characters in length.
IP Type	Specifies the IP type of the SLA Profile as IPv4 or IPv6. The default type is IPv4.
Detect Type	Specifies the detection type, including passive detection mode and active detection mode: • Passive - The passive detection mode samples TCP traffic on outbound links to obtain quality parameters such as latency, jitter, and packet loss rate of the links. This mode is the default mode.

Option	Description
	• Active - In active detection mode, the outbound interface of the link actively sends detection packets to specified destination addresses to obtain quality parameters such as latency, jitter, and packet loss rate of the links. When you select this mode, you need to specify the protocol type, destination address, detection interval, and number of sent packets for detection packets in subsequent configuration items.
Protocol	Specifies the protocol type for sending detection packets in active detection mode, which can be ICMP (ICMPV6) or TCP, with ICMP (ICMPV6) being the default. When you select TCP, you need to enter a TCP port number.
Address Type	Specifies the destination address for detection packets in active detection mode, which can be an IP address or a domain name. Once specified, you need to enter an IPv4 (IPv6) address or domain name in the corresponding field.
Detect Interval	Specifies the interval of sending detection packets in active detection mode. Valid values: 2 to 5 seconds. Default value: 2 seconds.
Packages Number	Specifies the number of detection packets to be sent in a single transmission in active detection mode. Valid values: 5 to 10. Default value: 5.
SLA Threshold	

Option	Description
Delay Threshold	Specifies the SLA delay threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no delay detection of link is performed.
Jitter Threshold	Specifies the SLA jitter threshold. Valid values: 0 to 100000 ms. Default value: 5. 0 indicates that no jitter detection of link is performed.
Loss Threshold	Specifies the SLA packet loss rate threshold. Valid values: 0 to 100 (0%-100%). Default value: 5. 0 indicates that no packet loss rate detection of link is performed.
Link Status	
Success Times Required For Activation	Specifies the number of successful activations required for a link to transition from inactive to active status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics falls below the configured threshold, the number of successful activations for the link increases by 1. When the cumulative activation count exceeds or equals the specified number of successful activations, the link transitions from inactive to active status, becoming an available outbound link. Valid values: 1 to 100. Default value: 5.
Failed Times Required For Inactivation	Specifies the number of failed deactivations required for a link to transition from active to inactive status. The system compares the detected link latency, jitter, and packet loss rate with the configured SLA thresholds. When any of these metrics exceeds

Option	Description
	the configured threshold, the number of failed deactivations for the link increases by 1. When the cumulative deactivation failure count exceeds or equals the specified number of failed deactivations, the link transitions from active to inactive status, becoming an unavailable outbound link. Valid values: 1 to 100. Default value: 5.

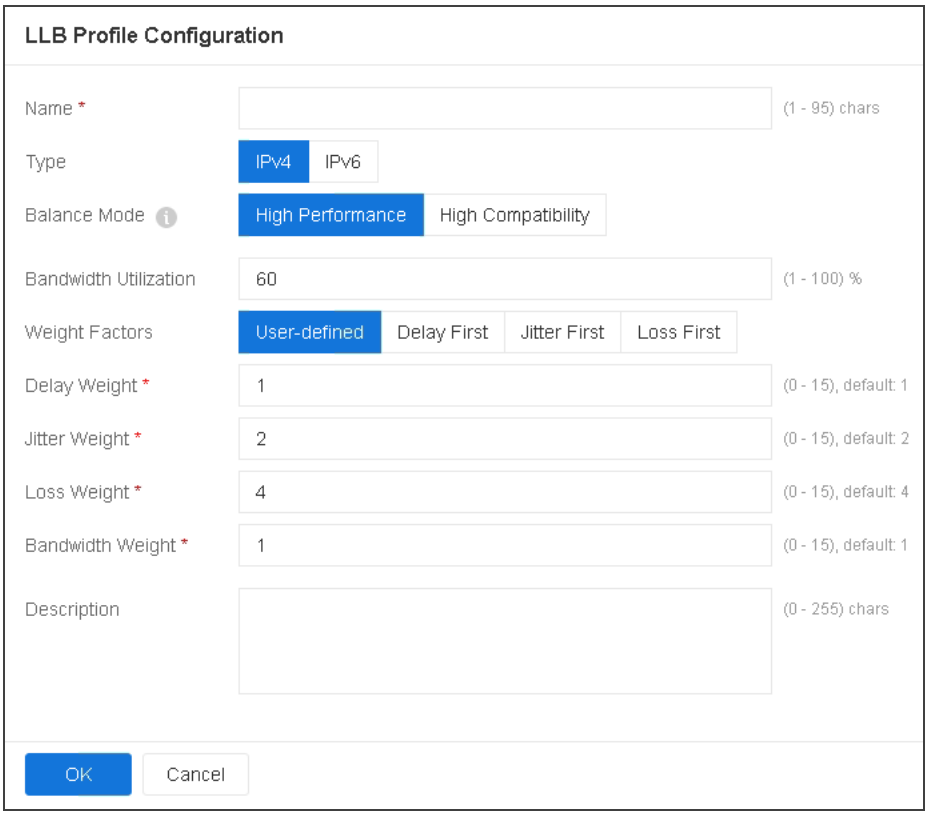
11. Click **OK**.
12. On the **SLA Profile** page, you can also perform the following operations:
    - Disable SLA profile: By default, a configured SLA profile is enabled. You can select one or more SLA profiles as required and click **Disable**. This way, these SLA profiles cannot be used for link quality detection and outbound path selection.
    - Enabling SLA profile: Select one or more SLA profiles as required and click **Enable** to enable them.
    - Edit SLA profile: Select an SLA profile and click **Edit** to edit the profile.
    - Delete SLA profile: Select one or more SLA profiles and click **Delete** to delete them.

Configuring LLB Profile

To configure an LLB profile, take the following steps:

1. Select **Network > Outbound LLB > LLB Profile**.

2. Click **New**.



3. In the LLB Profile Configuration page, configure as follows:

Option	Description
Name	Specifies the LLB Profile name whose length range is 1-95 characters.
Type	Specifies the IP type of the LLB Profile as IPv4 or IPv6. The default type is IPv4.
Balance Mode	There are two equalization modes: High Performance and High Compatibility. • High Performance - In this mode, system adjusts link to keep the link balance as fast as possible

Option	Description
	• High Compatibility - When the link load changes, system does not switch the link frequently, but ensures that the service is as far as possible on the previous link. This mode is suitable for services that are sensitive to link switching, such as banking services, only when the previous link is overloaded.
Bandwidth Utilization	Specifies the bandwidth utilization threshold of the interface. When the rate does not exceed the threshold by the interface bandwidth, the system will only analysis delay, jitter and packet loss rate to dynamically adjust the routing link; when the rate exceeds the threshold by the interface bandwidth, system will analysis of each link bandwidth utilization rate of the parameters at the same time to adjust the routing method. Value ranges from 0 to 100 (0% to 100%) and defaults to 60.
Weight Factors	The system selects routes based on the Cost value of each link, where a smaller Cost value indicates a more favorable link. "Weight Factors" is used to calculate the Cost value of a link, including parameters such as latency, jitter, packet loss rate, and bandwidth weight. These factors indicate the proportion of weight that latency, jitter, packet loss rate, and bandwidth have on the Cost value of the link. The weight factors of the Cost value of a link include the following options: • User-defined: You can customize the weight of latency, jitter, packet loss rate, and bandwidth of link. When you

Option	Description
	select this option, you need to specify the weight of latency, jitter, packet loss rate, and bandwidth for the Cost value of the link in subsequent configuration items. • Delay First: In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 10, 2, 4, and 1, respectively, indicating that latency has the greatest impact on the Cost value of the link. • Jitter First: In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 1, 10, 4, and 1, respectively, indicating that jitter has the greatest impact on the Cost value of the link. • Loss First: In this option, the weight for latency, jitter, packet loss rate, and bandwidth are 1, 2, 10, and 1, respectively, indicating that packet loss rate has the greatest impact on the Cost value of the link.
Delay Weight	Specifies the proportion of weight that latency has on the Cost value of the link. Valid values: 0 to 15. Default value: 1.
Jitter Weight	Specifies the proportion of weight that jitter has on the Cost value of the link. Valid values: 0 to 15. Default value: 2.
Loss Weight	Specifies the proportion of weight that packet loss rate has on the Cost value of the link. Valid values: 0 to 15. Default value: 4.
Bandwidth	Specifies the proportion of weight that bandwidth has on the

Option	Description
Weight	Cost value of the link. Valid values: 0 to 15. Default value: 1.
Description	Configure Additional details for the LLB profile.

4. Click **OK**.

5. On the **LLB Profile** page, you can also perform the following operations:

    - Edit LLB profile: Select an LLB profile and click **Edit** to edit the profile.
    - Delete LLB profile: Select one or more LLB profiles and click **Delete** to delete them.



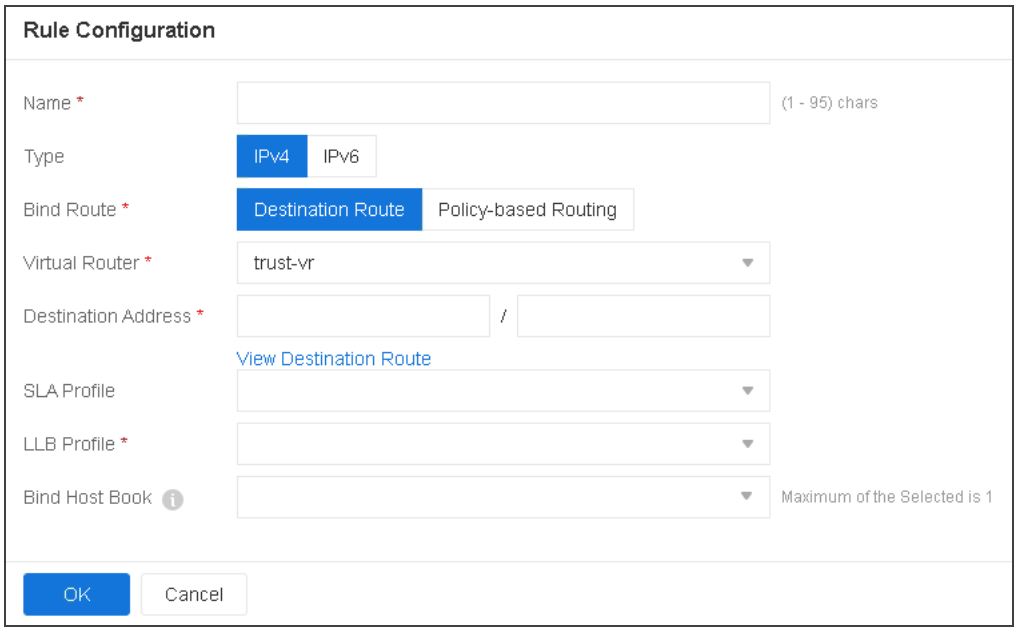
Notes: Changing the IP type is not allowed when editing the LLB Profile.

Configuring LLB Rule

To bind SLA profile (optional) and LLB profile to the route to form an LLB rule, which can control and load balance outbound link traffic, take the following steps:

1. Select **Network > Outbound LLB > Rule**.

2. Click **New**.



3. In the LLB Policy Configuration page, configure the following:

Option	Description
Name	Specifies the Rule name, length of 1-96 characters
Type	Specifies the type of the LLB Rule as IPv4 or IPv6. The default type is IPv4.
Bind Route	Specify the route to be bound in the rule: Destination Route or Policy Based Route. • Destination Route - When this option is selected, specify the virtual router and destination address of the destination route. • Policy Based Routing - Select this option to specify the name and id of the policy route. The IP type of PBR rule

Option	Description
	should be the same as the LLB Rule. If the IP tyoe of LLB Rule is IPv6, the IP type of PBR rule should be IPv6 as well.
Virtual Router	Specifies the name of the virtual router in the drop-down menu. The default vrouter is trust-vr.
Destination Address	Specifies the Vrouter destination address. When the type of the LLB Rule is specifies as IPv6, use *X:X:X:X::X/M* to configure the destination address of Vrouter. When the type of the LLB Rule is specifies as IPv4, the device supports two modes, A.B.C.D / M or A.B.C.D A.B.C.D, for example, 1.1.1.0/24 or 1.1.1.0 255.255.255.0.
SLA Profile	Select SLA Profile to bind. When the type of the LLB rule is specifies as IPv4, only the SLA Profile of IPv4 can be bound. When the type of the LLB Rule is specified as IPv6, only the SLA Profile of IPv6 can be bound.
LLB Profile	Select LLB Profile to bind. When the type of the LLB Rule is specified as IPv4, only the LLB Profile of IPv4 can be bound. When the type of the LLB Rule is specified as IPv6, only the LLB Profile of IPv6 can be bound. This item is required.
Bind Host Book	Select the host book when destination route is specified.

4. Click **OK**.

5. On the **Rule** page, you can also perform the following operations:

    - Delete LLB rule: Select one or more LLB rules and click **Delete** to delete them.
    - Filter LLB rule: Click **Filter**. Select a filter condition from the drop-down list and enter a value. This way, rules that meet the filter condition are displayed in the list. Repeat the steps above to add more filter conditions. The logical operator among these filter conditions is AND.

Inbound Link Load Balancing

After enabling the LLB for inbound traffic, the system will resolve domains of different IPs based on the sources of the DNS requests and return IPs for different ISPs to the corresponding users who initiate the requests, which reduces access across ISPs. Such a resolution method is known as SmartDNS.

You can enable inbound LLB by the following steps:

1. Enable SmartDNS. This is the prerequisite for the implementation of inbound LLB.
2. Configure a SmartDNS rule table. The smart domain-to-IP resolution is implemented based on the rule table.

Configuring Inbound Link Load Balancing

Before you start

- **Read** "Inbound Link Load Balancing" on Page 337

Creating a Smart DNS Rule Table

To create a SmartDNS rule table, take the following steps:

1. Select **Network > Inbound LLB**.
2. Click **New > Domain Table**.
3. In the Domain Configuration page, type a domain table name into Domain Table text box.
4. Type a domain name into Domain text box. Separate multiple domain names with comma. Each rule table supports up to 64 domain names (case insensitive).
5. Click **OK**.

6. In the Inbound LLB page, click the domain table name you already created and then click **New**.



Option	Description
ISP Static Address	Select a predefined or user-defined ISP from the drop-down list. If the source address matches any address entry of the ISP, system will return the specified IP.
Return IP	Specifies the return IP for different request sources. You can configure up to 64 IPs for a domain name.
Weight	Specifies the weight of the return IP. The value range is 1 to 100. The default value is 1. In the SmartDNS rule table, one domain name might correspond to multiple IPs. System will sort the IPs based on the weight and then return to the users.
Inbound Interface	Specifies the inbound interface for the return IP address. System will judge whether the return IP address is valid according to the track result or the protocol status of the inbound interface. Only the valid IP address will be returned to the request source. Select the proximity address to which the request source address will be matched from the drop-down list.
Track Object	Select a track object of interface type from the drop-down list. When the track object fails, the return IP address is invalid.

Option	Description
	When there's track object configured on the inbound interface, if the track status is successful, the return IP address is valid. Otherwise the IP address is invalid. When there's no track object configured on inbound interface, if the protocol state of the interface is UP, the return IP address is valid. Otherwise the IP address is invalid. If you don't specify the inbound interface for the return IP address, the return IP address is always valid.

7. Click **OK**.



Notes: The ISP route being referenced by the SmartDNS rule table cannot be deleted.

Application Layer Gateway (ALG)

Some applications use multi-channels for data transmission, such as the commonly used FTP. In such a condition the control channel and data channel are separated. Devices under strict security policy control may set strict limits on each data channel, like only allowing FTP data from the internal network to the external network to transfer on the well-known port TCP 21. Once in the FTP active mode, if a FTP server in the public network tries to initiate a connection to a random port of the host in the internal network, devices will reject the connection and the FTP server will not work properly in such a condition. This requires devices to be intelligent enough to properly handle the randomness of legitimate applications under strict security policies. In FTP instances, by analyzing the transmission information of the FTP control channel, devices will be aware that the server and the client reached an agreement, and open up a temporary communication channel when the server takes the initiative to connect to a port of the client, thus assuring the proper operation of FTP.

The system adopts the strictest NAT mode. Some VoIP applications may work improperly after NAT due to the change of IP address and port number. The ALG mechanism can ensure the

normal communication of VoIP applications after the NAT. Therefore, the ALG supports the following functions:

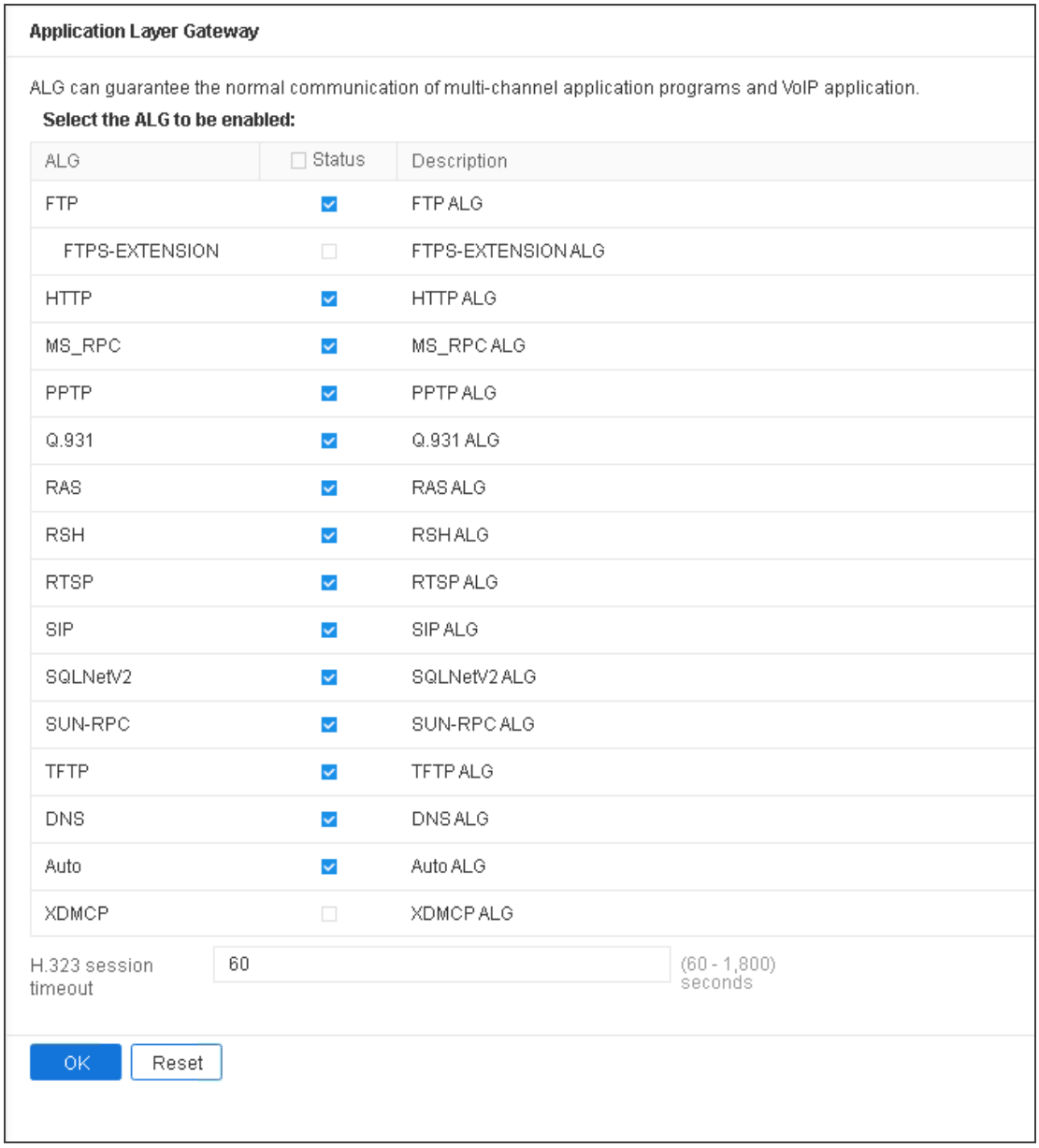
- Ensures normal communication of multi-channel applications under strict security policy rules.
- Ensures the proper operation of VoIP applications such as SIP and H.323 in NAT mode, and performs monitoring and filtering according to policies.

Enabling ALG

The system allows you to enable or disable ALG for different applications. Devices support ALG for the following applications: FTP, HTTP, MSRPC, PPTP, Q.931, RAS, RSH, RTSP, SIP, SQLNetV2, SUNRPC, TFTP, DNS, Auto and XDMCP. You can not only enable ALG for applications, but also specify H323's session timeout.

To enable the ALG for applications, take the following steps:

1. Select **Network> Application Layer Gateway**.
2. In the Application Layer Gateway dialog, select the applications that require ALG.



3. To modify H323's session timeout, type the value into the **H323 session timeout** box. The value range is 60 to 1800 seconds. The default value is 60.

4. Click **OK** to save your changes.

Notes: Only when the FTP ALG is enabled can the FTPS ALG be selected.

Enabling/Disabling DNS Rewrite by DNAT

After the device is enabled with the DNS ALG function, if the client initiates a DNS request, the DNS response message returned by the DNS server will prioritize matching DNAT rules, and will match DNS rewrite rules only if DNAT rule matching fails. In this case, the DNS response message may mistakenly match DNAT rules when it only needs to match DNS rewrite rules, resulting in abnormal service access.

To avoid abnormal service access, the system supports to enable/disable the DNS Rewrite by DNAT function. By default, this function is enabled. In other words, DNS response messages prioritize matching DNAT rules, and DNS rewrite rules will be matched only if DNAT rule matching fails. If this function is disabled, DNS response messages will only match DNS rewrite rules.

To enable/disable the DNS Rewrite by DNAT function, take the following steps:

1. Select **Network** > **Application Layer Gateway**.
2. Select the check box corresponding to DNS ALG to enable this function. After this function is enabled, "DNS Rewrite By DNAT" is displayed below. By default, this option is selected.
3. To disable the DNS Rewrite By DNAT function, unselect the option. After this function is disabled, DNS response messages will only match DNS rewrite rules.

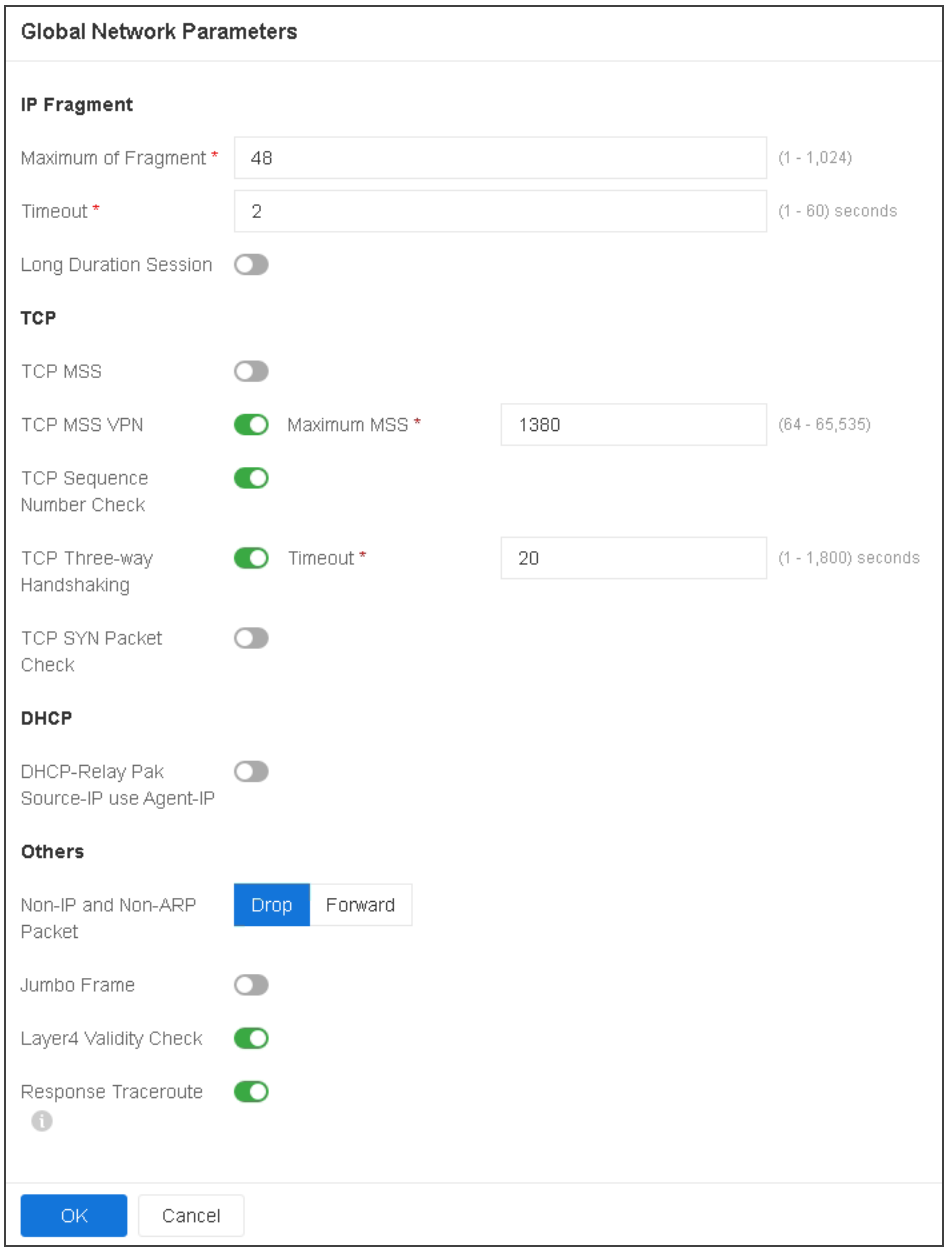
Global Network Parameters

Global network parameter configuration includes IP fragment, TCP packet processing methods and other options.

Configuring Global Network Parameters

To configure global network parameters, take the following steps:

1. Select **Network > Global Network Parameters > Global Network Parameters.**



2. Configure the following parameters.

Option	Description
IP Fragment	

Option	Description
Maximum Fragment Number	Specifies a maximum fragment number for every IP packet. The value range is 1 to 1024. The default value is 48. Any IP packet that contains more fragments than this number will be dropped.
Timeout	Specifies a timeout period of fragment reassembling. The value range is 1 to 60. The default value is 2. If the Hillstone device has not received all the fragments after the timeout, the packet will be dropped.
Long Duration Session	Enables or disables long duration session. If this function is enabled, specify long duration session's percentage in the Percentage text box below. The default value is 10, i.e., 10% of long duration session in the total sessions.
TCP	
TCP MSS	Specifies a MSS value for all the TCP SYN/ACK packets. Click the **Enable** button, and type the value into the Maximum MSS text box below.
Maximum MSS	Type the max MSS value into the Maximum MSS text box below. The value range is 64 to 65535. The default value is 1448.
TCP MSS VPN	Specifies a MSS value for IPSec VPN's TCP SYN packets. Click the **Enable** button, and type the value into the Maximum MSS text box below.
Maximum MSS	Type the max MSS value for IPSEC VPN into the Maximum MSS text box below. The value range is 64 to 65535. The default value is 1380.

Option	Description
TCP Sequence Number Check	Configures if the TCP sequence number will be checked. When this function is enabled, if the TCP sequence number exceeds TCP window, that TCP packet will be dropped.
TCP Three-way Hand-shaking	Configures the function of TCP three-way handshaking. Click the **Enable** button to enable this function, and specify a timeout value in the Timeout text box below. The value range is 1 to 1800 seconds. The default value is 20. If the three-way hand-shaking has not been completed after timeout, the connection will be dropped.
TCP SYN Packet Check	Click the **Enable** button to enable this function and specify the action for TCP non-SYN packet. When the received packet is a TCP SYN packet, the TCP connection will be established. When the received packet is a TCP non-SYN packet, the packet will be processed according to the specified action. • drop: When the received packet is a TCP non-SYN packet, the system will drop the packet. • reset: When the received packet is a TCP non-SYN packet, the system will drop the packet and send RST packet to the peer device.
DHCP	
DHCP-Replay Pak Source IP	Click the button to enable this function. This way, when the device acts as a DHCP relay proxy, the source IP of the DHCP relay packets is replaced with the agent IP, and the

Option	Description
use Agent-IP	source port of the packets is changed to 67. By default, this function is disabled, indicating that the source IP of the DHCP relay packets is the IP address of the egress interface and the source port of the packets is 68.
Application Layer	
Application Layer Fast Forward	Click the button to enable this function. This way, when only the Intrusion Prevention function at the application layer is enabled and the protocol max scan length configured in the intrusion prevention rule is reached, traffic at the application layer will no longer be forwarded to the SSM module or CPU for parsing and processing. This enhances the device performance. By default, this function is disabled. **Note**: Only SG-6000-A7600/A6800 devices support this function.
Others	
Non-IP and Non-ARP Packet	Specifies how to process packets that are neither IP nor ARP.
Jumbo Frame	Click the **Enable/Disable** button to enable or disable the Jumbo Frame function. This function is disabled by default. With the Jumbo Frame function enabled, the system can forward packets less than or equal to 9216 bytes as follows: • For IPv4/IPv6 packets that are less than the MTU value of the outbound interface, forward them directly.

Option	Description
	• For IPv4 packets that are larger than the MTU value of the outbound interface, the packets are forwarded in fragments. • For IPv6 packets that are larger than the MTU value of the outbound interface, an "ICMPv6 Packet Too Big" error message will be sent to the source node of the packets, and the sender is urged to shorten the length of the packets.  Notes: • When the Jumbo Frame function is enabled, the MTU configuration range of the interface will be changed. For more information about the MTU value configuration of the interface, see Configuring an Interface. • SG-6000-A7600/A6800 does not support the Jumbo Frame function.
Layer4 Validity Check	Enable/Disable validity check for Layer 4 protocol. By default, this function is enabled. Layer 4 indicates the transport layer of the OSI model, which provides end-to-end communication between devices and ensures the integrity of data transmission. When this function is enabled, the system checks TCP packets

Option	Description
	at Layer 4, such as checking whether the flag of TCP is valid and whether the port number is valid. If the TCP packet is abnormal, it will be dropped.
Response Traceroute	Enable/Disable the Response Traceroute function. By default, this function is enabled. By default, the system will respond to traceroute traffic passing through the device. When the traceroute traffic is not sent or received by the device itself, you can disable the Response Traceroute function to prevent the device from responding to traceroute traffic that does not belong to the device itself. This way, the IP address of the device is hidden, which reduces the possibility of the device being discovered and attacked. **Note:** This parameter takes effect only for traceroute traffic that does not belong to the device itself. For traceroute traffic that does not belong to the device itself, whether this function is enabled does not affect the response of the device to the traffic.

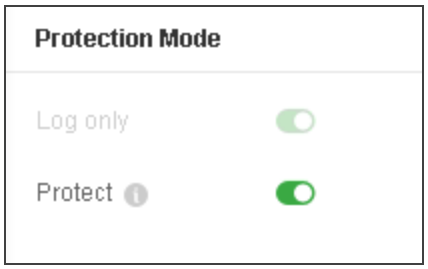
3. Click **OK**.

Configuring Protection Mode

To configure the protection mode, take the following steps:

1. Select **Network > Global Network Parameters > Protection Mode**.

2. Configure the traffic working mode.



   - Log only - System only generates protocol anomaly alarms and attacking behavior logs, but will not block attackers or reset connections.
   - Protect - System not only records attack behavior detected by Intrusion Prevention System, Anti-Virus or AD, Policy, Black list, but also reset the connection or block the access.

Notes: Log & reset mode is recommended. In this mode, the security performance of the device can take effect normally. If log only mode is selected, system can only record logs, and functions which can block traffic in system will be invalid, including policy, IPS, AV, QoS, etc.

IPv6 Tunnel

IPv6 over IPv4 Tunnel

At the time of writing IPv4 networks are still mainstream networks, while IPv6 networks are comparatively isolated. IPv6 over IPv4 tunnel allows IPv6 packets to be transmitted via IPv4 networks, enabling communication between isolated IPv6 networks via IPv4 networks. The system supports to configure the following IPv6 over IPv4 tunnels:

- Configuring an Automatic 6to4 Tunnel
- Configuring a Manual 6to4 Tunnel

- Configuring an ISATAP Tunnel
- Configuring a 6RD Tunnel

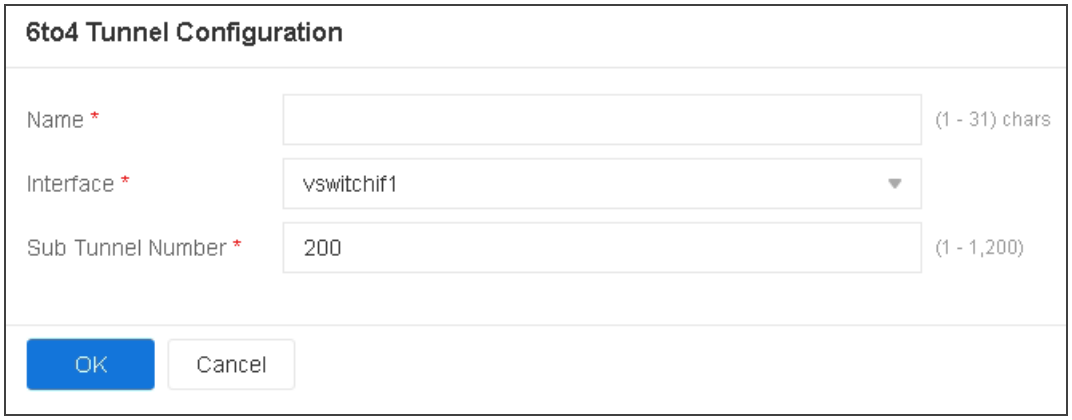
Notes: The configured IPv6 over IPv4 tunnel will only take effect after being bound to the Tunnel Interface.

Configuring an Automatic 6to4 Tunnel

Automatic 6to4 tunnel is an automatic one-to-many tunnel that is used to connect multiple isolated IPv6 networks via IPv4 networks. Hillstone devices can either be used as 6to4 routes or 6to4 relay routers, specifically relying on network environment.

To create an IPv6 automatic 6to4 tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **6to4 Tunnel** tab.
3. Click **New**.



Option	Description
Name	Specifies the name of the automatic 6to4 tunnel.
Interface	Specifies the name of egress interface which can be a physical interface or logical interface (except for tunnel interface). Select

Option	Description
	the interface from the drop-down list or you can click ⊕ to create an interface.
Sub Tunnel Number	Specifies the subtunnel number of a automatic 6to4 tunnel. The value rang is 1 to 1,200, and the default value is 200. Each automatic 6to4 tunnel can have a maximum of 1,200 sub-tunnels.

4. Click **OK**.

To edit an automatic 6to4 tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **6to4 Tunnel** tab.
3. Select the automatic 6to4 tunnel that you want to edit.
4. Click **Edit**. On the **6to4 Tunnel Configuration** page, make changes as needed.

To delete an automatic 6to4 tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **6to4 Tunnel** tab.
3. Select the automatic 6to4 tunnel that you want to delete.
4. Click **Delete**.

Configuring a Manual 6to4 Tunnel

Manual 6to4 tunnel provides point-to-point connection. The end point of the tunnel is manually configured.

To create an IPv6 manual 6to4 tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select **Manual Tunnel** tab.
3. Click **New**.



Option	Description
Name	Specifies the name of the manual 6to4 tunnel.
Interface	Specifies the name of egress interface which can be a physical interface or logical interface (except for tunnel interface). Select the interface from the drop-down list or you can click ⊕ to create an interface.
Destination IP	Specifies a destination address for the IPv6 manual 6to4 tunnel. This address is an IPv4 address.

4. Click **OK**.

To edit a manual 6to4 tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **Manual Tunnel** tab.

3. Select the manual 6to4 tunnel that you want to edit.
4. Click **Edit**. On the **Manual Tunnel Configuration** page, make changes as needed.

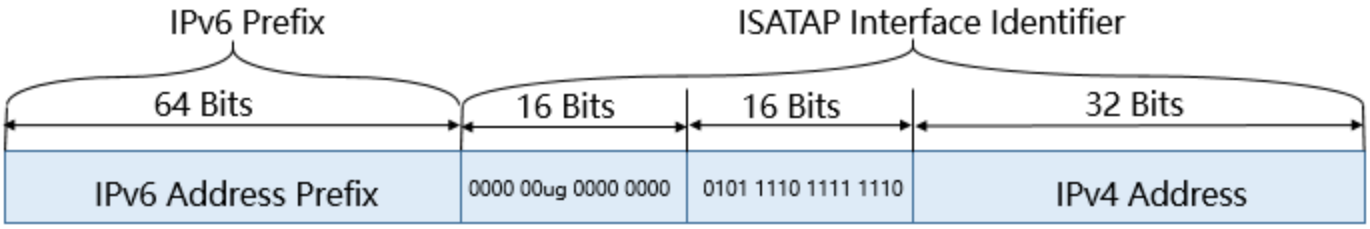
To delete a manual 6to4 tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **Manual Tunnel** tab.
3. Select the manual 6to4 tunnel that you want to delete.
4. Click **Delete**.

Configuring an ISATAP Tunnel

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol) is a auto tunnel technology of IPv6 point-to-multipoint. It's mainly used for the dual-stack host in the IPv4 networks to visit IPv6 networks. With the technology, the dual-stack host can obtain the terminal of tunnel automatically via the embedded IPv4 address in the destination address of IPv6 packets.

When ISATAP tunnel is built, both the destination address of IPv6 packets and IPv6 address of the tunnel interface need the special ISATAP address. The ISATAP address contains the IPv6 prefix and ISATAP interface identifier. The formats of ISATAP address are as follows:



- If the IPv4 address is globally unique, the **u** bit is 1, otherwise, it is 0.
- The **g** bit means an IEEE (Institute of Electrical and Electronic Engineers) group or individual ID, which is 0 all the time.

For example, the prefix of IPv6 is 2001:DB8:1234:5678::/64 and the IPv4 address needs to be embedded is 10.173.129.8, which can be identified as 0AAD:8108 (hexadecimal), the ISATAP address is 2001:DB8:1234:5678:0000:5EFE: 0AAD:8108.

To create a new ISATAP tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **ISATAP Tunnel** tab.
3. Click **New**.



Option	Description
Name	Specifies the name of the ISATAP tunnel.
Interface	Specifies the name of egress interface which can be a physical interface or logical interface (except for tunnel interface). Select the interface from the drop-down list or you can click ⊕ to create an interface.
Sub Tunnel Number	Specifies the subtunnel number of an ISATAP tunnel. The value rang is 1 to 1,200, and the default value is 200. Each ISATAP tunnel can have a maximum of 1,200 sub-tunnels.

4. Click **OK**.

To edit an ISATAP tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **ISATAP Tunnel** tab.
3. Select the ISATAP tunnel that you want to edit.
4. Click **Edit**. On the **ISATAP Tunnel Configuration** page, make changes as needed.

To delete an ISATAP tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **ISATAP Tunnel** tab.
3. Select the ISATAP tunnel that you want to delete.
4. Click **Delete**.

Configuring a 6RD Tunnel

6RD (IPv6 Rapid Deployment on IPv4 Infrastructures) is a stateless tunneling mechanism, allowing a service provider to quickly and securely deploy IPv6 without upgrading existing IPv4 access network infrastructures.

6RD builds on the 6to4 tunneling mechanism. It uses a service provider's own IPv6 prefix rather than the fixed prefix (2002::/16) of the automatic 6to4 tunnel. This not only resolves the IPv4 address exhaustion problem, but also conquers the disadvantage that automatic 6to4 tunnels use the fixed well-known IPv6 prefix on all 6to4 sites. From the perspective of customer sites and the IPv6 Internet at large, the IPv6 service provided is equivalent to native IPv6.

The IPv6 address of 6RD is composed of the delegated prefix and the subnet ID. The delegated prefix is calculated by combining the 6RD prefix and a consecutive set of bits from the IPv4 address. The 6RD prefix is obtained from a service provider, and the IPv4 bits are obtained from all or part of the IPv4 address. The number of IPv4 bits needed depends on the IPv4 prefix length configured for the 6RD tunnel.

The format of 6RD IPv6 address is as follows.

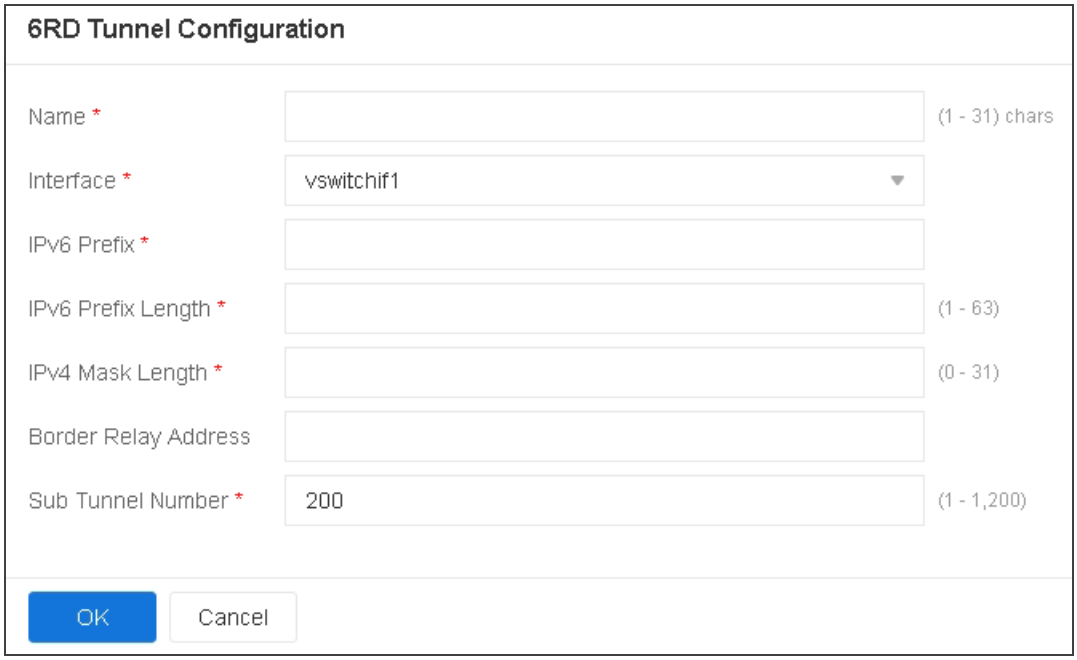


6RD application scenarios include:

- 6RD tunnel: 6RD can be used for interconnection between 6RD domains. A 6RD domain consists of 6RD CE (Customer Edge) routers and one or more 6RD BRs (Border Relays). Each 6RD domain uses a specific 6RD prefix. Devices on the two sides of a 6RD tunnel are both 6RD CEs or both 6RD BRs.
- 6RD relay: 6RD can be used for interconnection between a 6RD domain and an IPv6 native network. The device on one side of the 6RD tunnel is a 6RD CE, and on the other side is a 6RD BR.

To create a 6RD tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **6RD Tunnel** tab.
3. Click **New**.



Option	Description
Name	Specifies the name of the 6RD tunnel.
Interface	Specifies the name of egress interface which can be a physical interface or logical interface (except for tunnel interface). Select the interface from the drop-down list or you can click ⊕ to create an interface.
IPv6 Prefix	Specifies a 6RD prefix, which is used for matching 6RD packets. A 6RD prefix is assigned by a service provider.
IPv6 Prefix Length	Specifies the 6RD prefix lenght. The value ranges from 1 to 63.
IPv4 Mask Length	Specifies the IPv4 prefix length. The value ranges from 0 to 31.
Border Relay	Specifies the BR's IPv4 address. In the 6RD relay application

Option	Description
Address	scenario, when the destination IP address of 6RD packets fails to match the 6RD prefix, the BR's IPv4 address will be used as the destination IPv4 address of the outer-layer IPv4 packets.
Sub Tunnel Number	Specifies the maximum number of 6RD subtunnels. The value ranges from 1 to 1,200. The default value is 200.

4. Click **OK**.

To edit a 6RD tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **6RD Tunnel** tab.
3. Select the 6RD tunnel that you want to edit.
4. Click **Edit**. On the **6RD Tunnel Configuration** page, make changes as needed.

To delete a 6RD tunnel, take the following steps:

1. Select **Network** > **IPv6 Tunnel** > **IPv6 over IPv4 Tunnel**.
2. Select the **6RD Tunnel** tab.
3. Select the 6RD tunnel that you want to delete.
4. Click **Delete**.

Chapter 6 Advanced Routing

Routing is the process of forwarding packets from one network to the destination address in another network. Router, a packet forwarding device between two networks, is designed to transmit packets based on the various routes stored in routing tables. Each route is known as a routing entry.

Hillstone devices are designed with Layer 3 routing. This function allows you to configure routing options and forward various packets via VRouter. System implements with a default VRouter trust-vr, and also supports multiple VRouters (multi-VR).

Hillstone devices support destination routing, ISP routing, Source-Based Routing (SBR), Source-Interface-Based Routing (SIBR), Destination-Interface-Based Routing (DIBR), Policy-Based Routing (PBR), dynamic routing (including RIP, OSPF and BGP) and Equal Cost MultiPath Routing (ECMP).

- Destination Routing: A manually-configured route which determines the next routing hop according to the destination IP address.
- DIBR: A manually-configured route which determines the next routing hop according to the destination IP address and ingress interface.
- SBR: Source IP based route which selects routers and forwards data according to the source IP address.
- SIBR: Source IP and ingress interface based route.
- ISP Profile: Add a subnet to an ISP.
- ISP Routing: A kind of route which determines the next hop based on different ISPs.
- PBR: A route which forwards data based on the source IP, destination IP address and service type.

- Dynamic Routing: Selects routers and forwards data according to the dynamic routing table generated by dynamic routing protocols ("RIP" on Page 390, "OSPF" on Page 395 or BGP).
- ECMP: Load balancing traffic destined to the same IP address or segment in multiple routes with equal management distance.
- Configuring PIM/PIMv6: The Protocol Independent Multicast (PIM) indicates that static route or any unicast routing protocol, such as RIP, OSPF, IS-IS, or BGP, can provide the routing information for IP multicast. Multicast routing is not dependent on the unicast routing protocols, as long as the multicast routing tables are generated by the unicast routing protocols.

When forwarding the inbound packets, the device will select a route in the following sequence: PBR > SIBR > SBR > DIBR > Destination routing/ISP routing/Proximity routing/Dynamic routing.

Routing supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry for the routing rule.

Related Topics:

- "Destination Route" on Page 361
- "Destination-Interface Route" on Page 364
- "Source Route" on Page 367
- "Source-Interface Route" on Page 369
- "ISP Profile" on Page 375
- "ISP Route" on Page 372
- "Policy-based Route" on Page 378
- "RIP" on Page 390

Destination Route

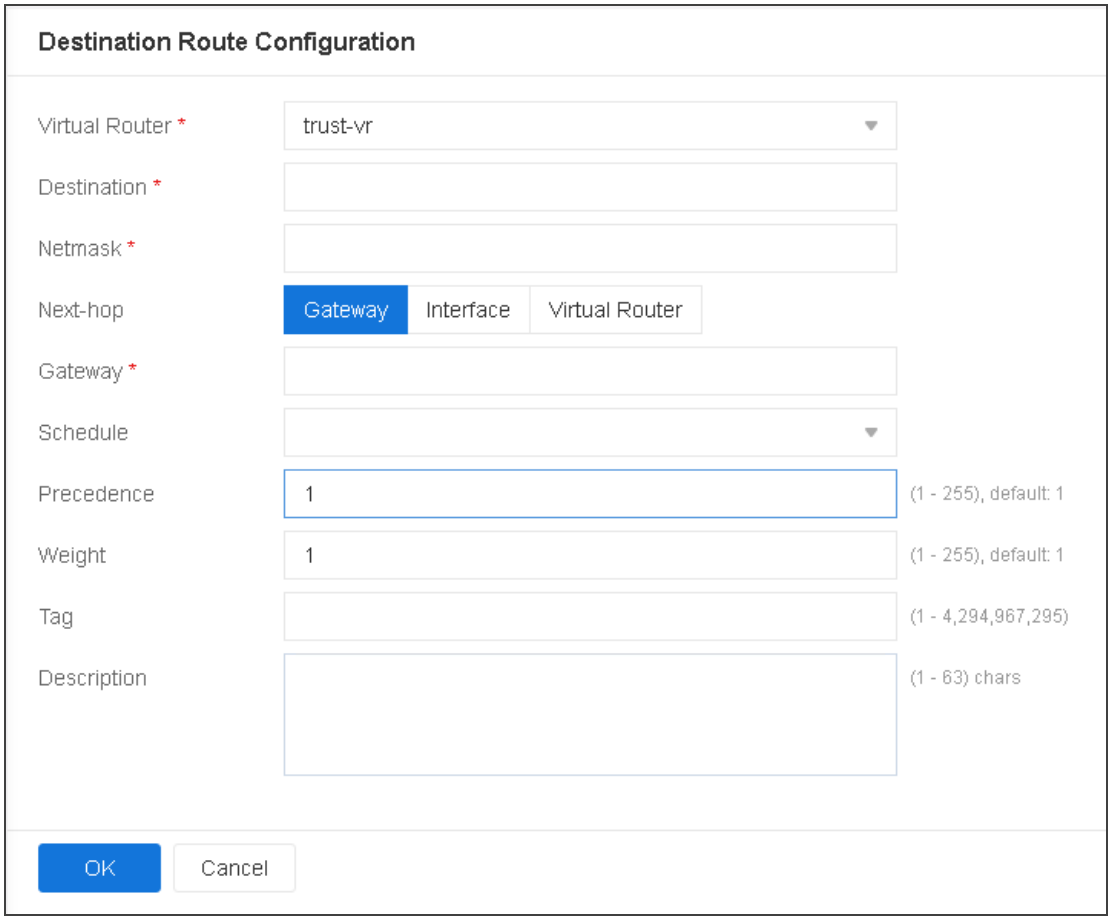
The destination route is a manually-configured route entry that determines the next routing hop based on the destination IP address. Usually a network with comparatively a small number of out-bound connections or stable Intranet connections will use a destination route. You can add a default route entry at your own choice as needed.

Creating a Destination Route

To create a destination route, take the follwing steps:

1. Select **Network** > **Routing** > **Destination Route**.
2. Select the IPv4 or IPv6 tab page, and create an IPv4 destination route or IPv6 destination route on the corresponding page. This step is only applicable for IPv6 version.
3. Click **New**.

   In the Destination Route Configuration page, enter values.



Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Routerouter for the new route. The default value is "trust-vr".
Destination	Type the IP address for the route into the text box.
Netmask	Type the corresponding subnet mask into the text box.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router**, **Interface**. • Gateway: Type the IP address into the **Gateway** text box. • Virtual Router: Select a name from the drop-down list.

Option	Description
	• Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Track Object	Select a created track object from the drop-down manual. When the track fails, the route will be invalid.
Precedence	Type the route precedence into the text box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the route into the text box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Tag	Specifies the tag value of the destination route. When OSPF redistributes routes, if the configured routing tag values here are matched to the rules in the routing mapping table, the route will be redistributed to filter its information. The value range is 1 to 4294967295.

Option	Description
Description	Type the description information into the Description text box if necessary.

4. Click **OK**.

Destination-Interface Route

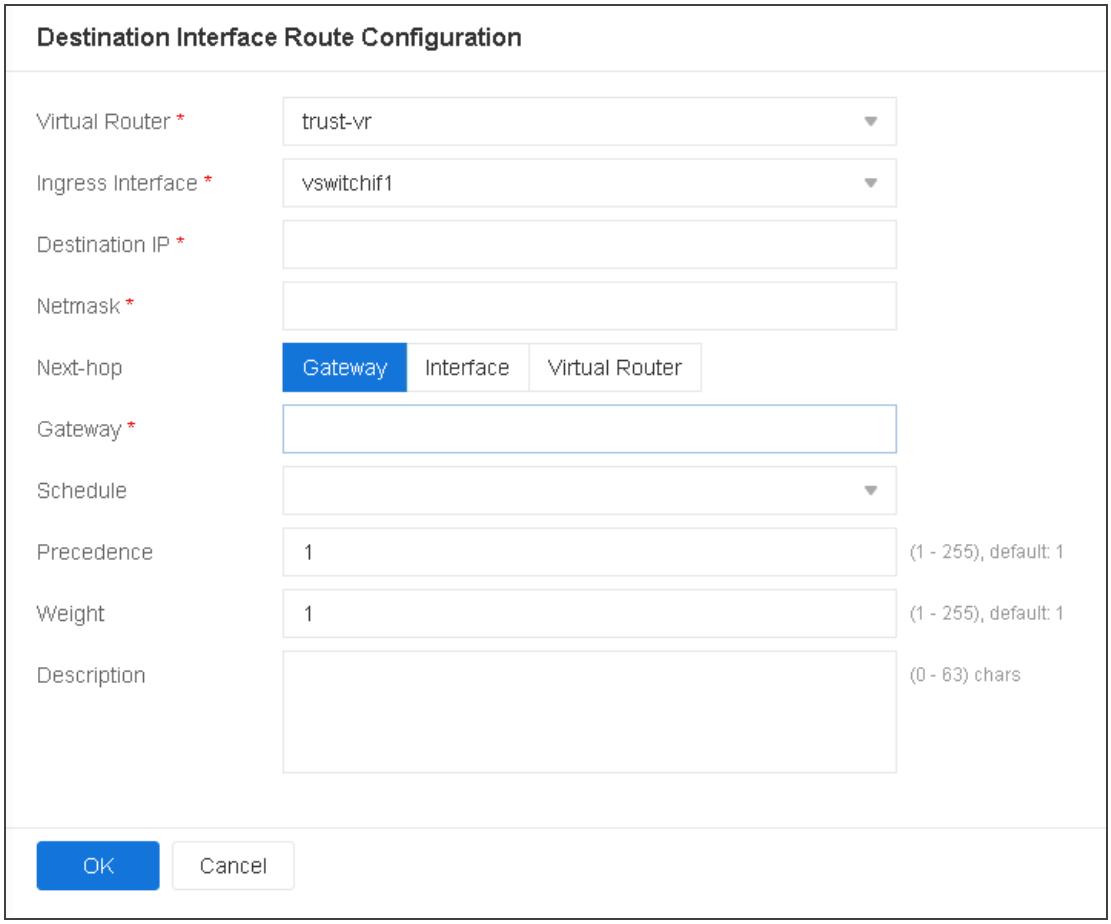
Destination interface route is designed to select a route and forward data based on the Destination IP address and ingress interface of a packet.

Creating a Destination-Interface Route

To create a Destination-Interface route, take the following steps:

1. Select **Network** > **Routing** > **Destination Interface Route**.
2. Select the IPv4 or IPv6 tab page, and create an IPv4 Destination-Interface route or IPv6 Destination-Interface route on the corresponding page. This step is only applicable for IPv6 version.
3. Click **New**.

   In the Destination Interface Route Configuration page, enter values.



Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Routerouter for the new route. The default value is "trust-vr".
Ingress Inter-face	Select an interface for the route from the drop-down list.
Destination IP	Type the Destination IP for the route into the textbox.
Netmask	Type the corresponding subnet mask into the textbox.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router**, **Interface**.

Option	Description
	• Gateway: Type the IP address into the **Gateway** text box. • Virtual Router: Select a name from the **Virtual Router** drop-down list. • Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Track Object	Select a created track object from the drop-down manual. When the track fails, the route will be invalid.
Precedence	Type the route precedence into the textbox. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the DIBR into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box

Option	Description
	if necessary.

4. Click **OK**.

Source Route

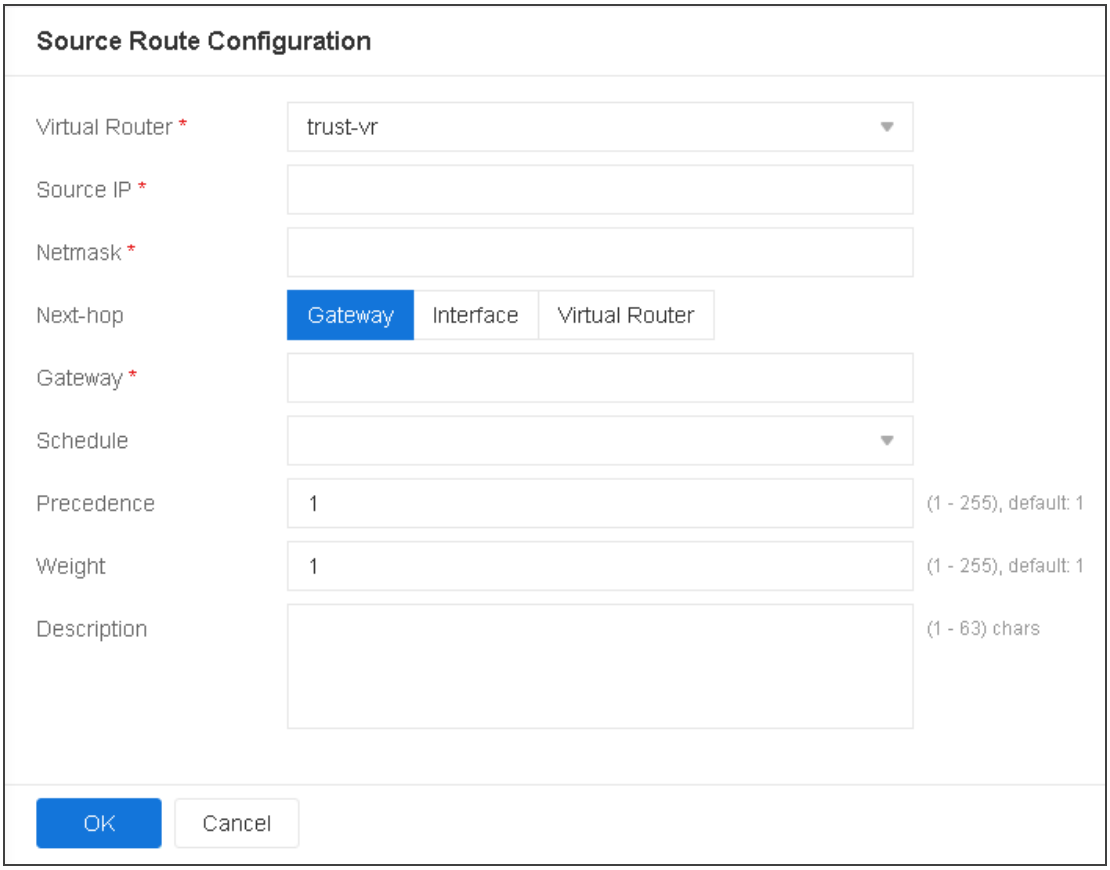
Source route is designed to select a router and forward data based on the source IP address of a packet.

Creating a Source Route

To create a source route, take the following steps:

1. Select **Network** > **Routing** > **Source Route**.
2. Select the IPv4 or IPv6 tab page, and create an IPv4 source route or IPv6 source route on the corresponding page. This step is only applicable for IPv6 version.
3. Click **New**.

   In the Source Route Configuration page, enter values.



Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Routerouter for the new route. The default value is "trust-vr".
Source IP	Type the source IP for the route into the box.
Netmask	Type the corresponding subnet mask into the box.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router**, **Interface**. • Gateway: Type the IP address into the **Gateway** text box. • Virtual Router: Select a name from the drop-down list.

Option	Description
	• Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Track Object	Select a created track object from the drop-down manual. When the track fails, the route will be invalid.
Precedence	Type the route precedence into the box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the route into the box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

4. Click **OK**.

Source-Interface Route

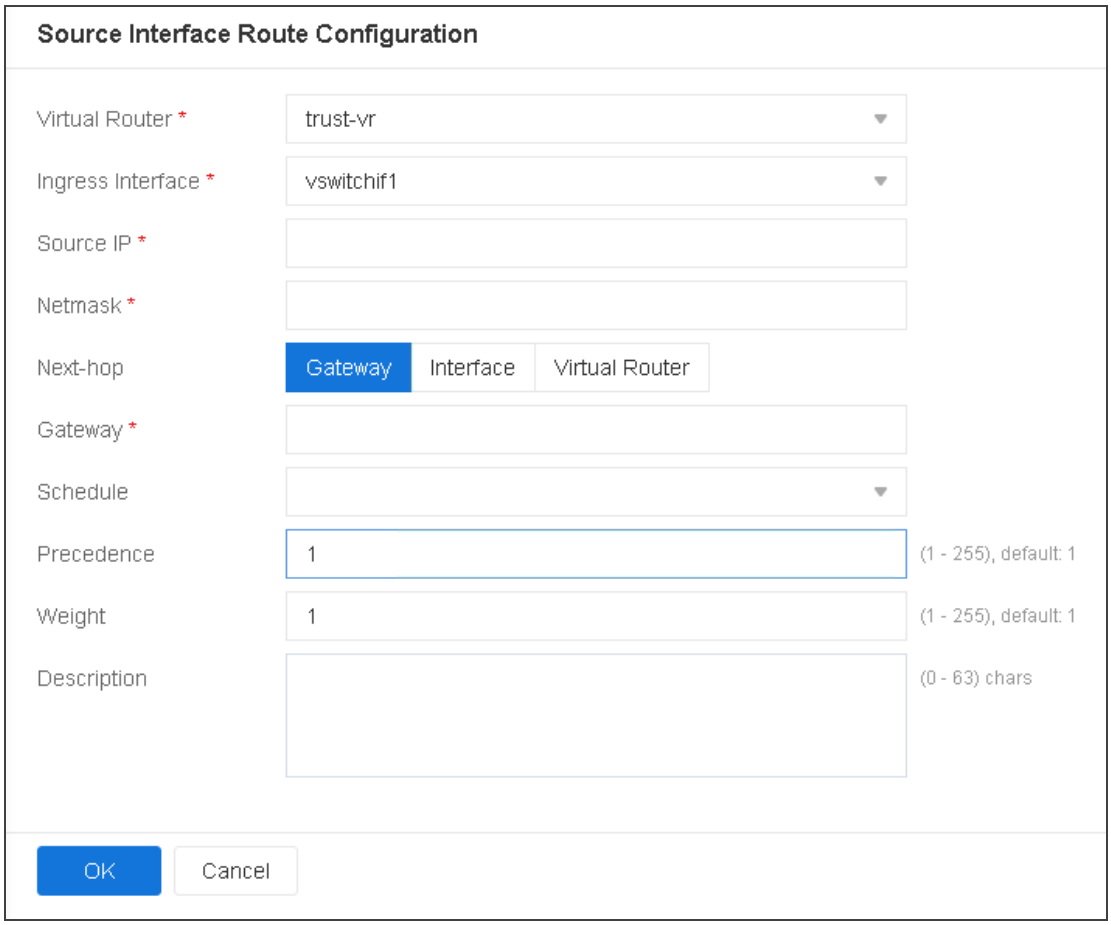
Source interface route is designed to select a router and forward data based on the source IP address and ingress interface of a packet.

Creating a Source-Interface Route

To create a Source-Interface route, take the following steps:

1. Select **Network** > **Routing** > **Source Interface Route**.
2. Select the IPv4 or IPv6 tab page, and create an IPv4 Source-Interface route or IPv6 Source-Interface route on the corresponding page. This step is only applicable for IPv6 version.
3. Click **New**.

   In the Source Interface Route Configuration page, enter values.



Option	Description
Virtual Router	From the Virtual Router drop-down list, select the Virtual Routerouter for the new route. The default value is "trust-vr".

Option	Description
Ingress Interface	Select an interface for the route from the drop-down list.
Source IP	Type the source IP for the route into the textbox.
Netmask	Type the corresponding subnet mask into the textbox.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router**, **Interface**. • Gateway: Type the IP address into the **Gateway** text box. • Virtual Router: Select a name from the **Virtual Router** drop-down list. • Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Track Object	Select a created track object from the drop-down manual. When the track fails, the route will be invalid.
Precedence	Type the route precedence into the textbox. The smaller the parameter is, the higher the precedence is. If multiple routes are

Option	Description
	available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the ISP route into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

4. Click **OK**.

ISP Route

Generally many users might apply for multiple lines for load balancing purpose. However, a typical balance will not have the function based on the traffic's direction. For such a scenario, the device provides the ISP route, which allows traffic from different ISPs to take their proprietary routes, thus accelerating network access.

To configure an ISP route, first you need to add a subnet to an ISP, and then configure the ISP route. The destination of the route is determined by the name of the ISP. You can customize ISP information, or upload and download custom profiles that contain different ISP information. You can implement remote or local update on pre-defined ISP profiles by using the ISP information database. By default, the system automatically updates the ISP information database on a daily basis. You can modify the update configuration as needed. For more information, see Updating Signature Database.

Creating an ISP Route

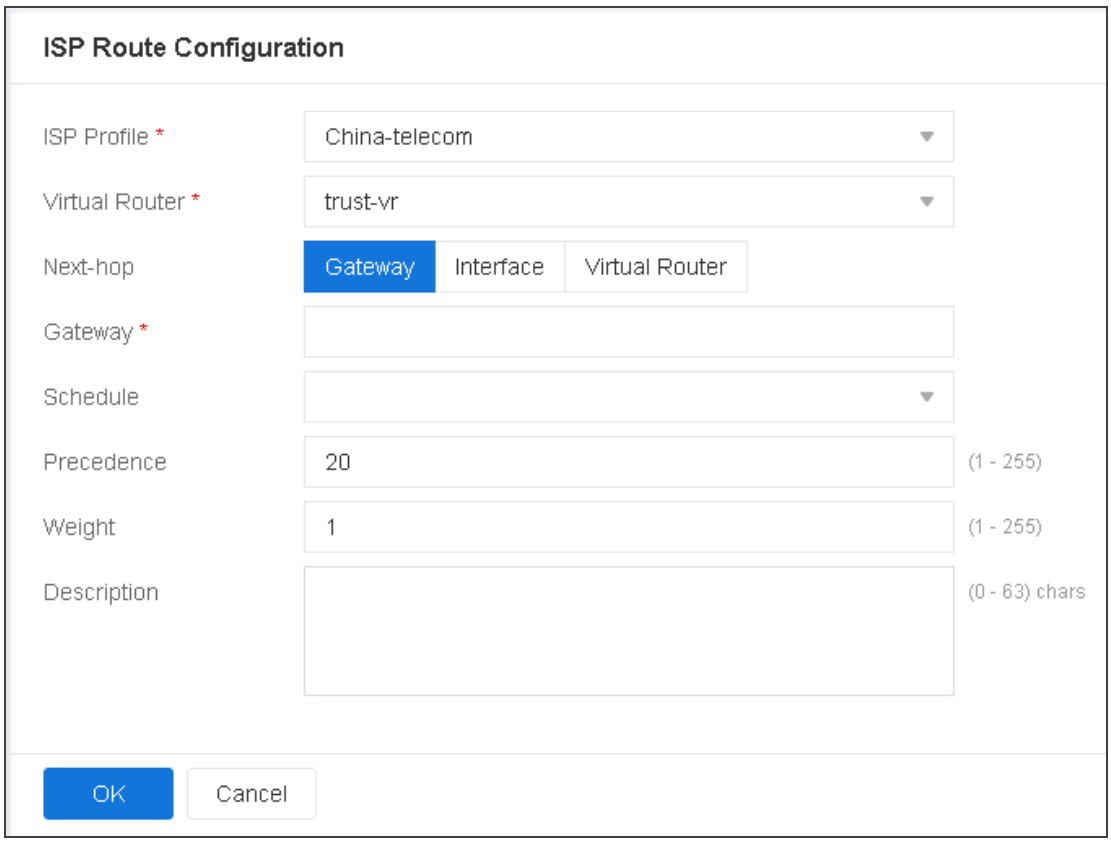
To create an ISP route, take the following steps:

1. Select **Network** > **Routing** > **ISP Route**.

2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.

3. Click **New**.

In the ISP Configuration page, enter values.



Option	Description
ISP Profile	Select an ISP profile name from the drop-down list.
Virtual Router	From the **Virtual Router** drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router**, **Interface**. • Gateway: Type the IP address into the **Gateway** text box.

Option	Description
	• Virtual Router: Select a name from the **Virtual Router** drop-down list. • Interface: Select a name from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. For a tunnel interface, you need to type the gateway address for the tunnel's peer in the optional box below.
Schedule	Specifies a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Precedence	Type the route precedence into the textbox. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 10. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the ISP route into the textbox. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the Description text box if necessary.

4. Click **OK**.

ISP Profile

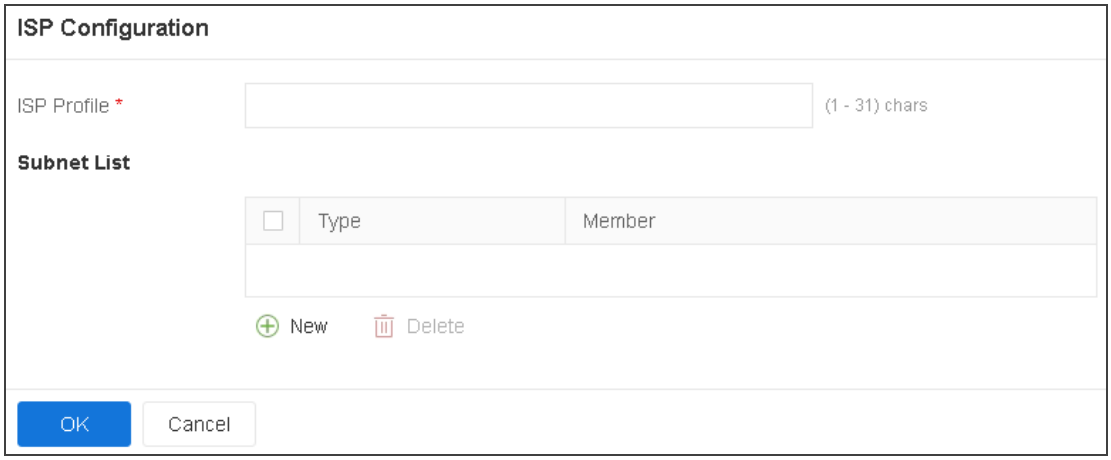
To configure an ISP route, you need to first add a subnet to an ISP, and then configure the ISP route. The destination of the route is determined by the name of the ISP. You can customize ISP information, or upload and download custom profiles that contain different ISP information. You can implement remote or local update on pre-defined ISP profiles by using the ISP information database. By default, the system automatically updates the ISP information database on a daily basis. You can modify the update configuration as needed. For more information, see Updating Signature Database.

Creating an ISP Profile

To create an ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version
3. Click **New**.

   In the ISP Configuration page, enter values.



Option	Description
ISP Profile	Type the name for the new ISP profile into the textbox.
Subnet List	

Option	Description
Member	Specifies the member type of the ISP profile, including subnet member entry and ISP profile member entry. When creating an IPv4 ISP profile: • Add subnet member: Select **IP/Netmask** from the drop-down list, and then type the IPv4 address and nermask for the subnet into the textbox. • Add an IPv4 ISP menber: Add an IPv4 ISP profile entry, that is to add other configured IPv4 ISP profile (pre-defined IPv4 ISP profile or user-defined IPv4 ISP profile), select **ISP Profile** from the drop-down list, and then select the ISP profile name. When creating an IPv6 ISP profile: • Add subnet member: Select **IPv6/Prefix** from the drop-down list, and then type the IPv6 address and prefix for the subnet into the textbox. • Add an IPv6 ISP menber: Add an IPv6 ISP profile entry, that is to add other configured IPv6 ISP profile (pre-defined IPv6 ISP profile or user-defined IPv6 ISP profile), select **ISP Profile** from the drop-down list, and then select the ISP profile name.
New	Add the member to the ISP profile. The member will be displayed in the list below. If needed, repeat the steps to add multiple subnets for the ISP profile.

Option	Description
Delete	Delete the selected ISP profiles.

4. Click **OK**.

Deleting a User-defined ISP Profile

To delete a user-defined ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version
3. Selete the user-defined ISP profile, and click **Delete**.

Notes:

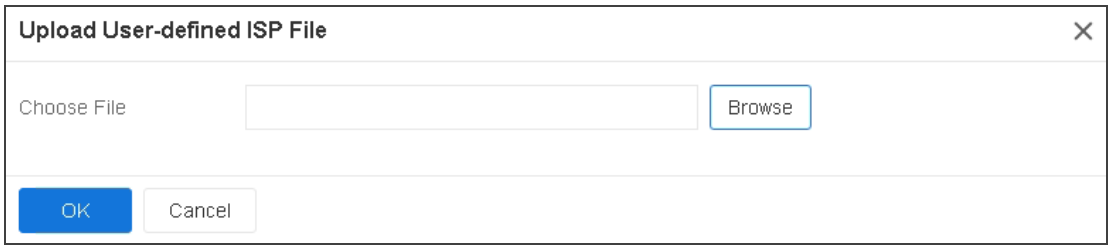
- The predefined ISP profile cannot be deleted.
- To ensure that the custom ISP profile can be deleted normally, please delete the nested ISP profile entry before deleting it.

Uploading a User-defined ISP Profile

To upload a user-defined ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.

3. Click **Upload**.



4. Click **Browse** to select the user-defined ISP profile in your PC.
5. Click **Upload** to upload the selected user-defined ISP profile to device.

Downloading an ISP Profile

To download an ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.
3. Click **Download**.
4. In the Download User Defined ISP File panel, select an ISP profile from the **ISP profile** drop-down list.
5. Click **OK** to download the profile to a specified location in PC.

Policy-based Route

Policy-based Route (PBR) is designed to select a router and forward data based on the source IP address, destination IP address and service type of a packet.

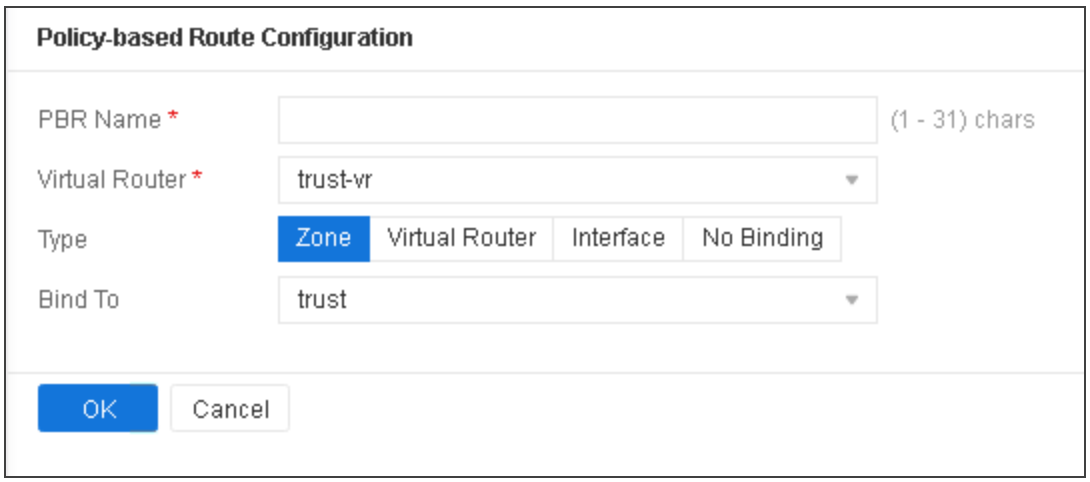
Creating a Policy-based Route

To create a Policy-based route, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **New**. Select **PBR** from the drop-down list.

   In the Policy-based Route Configuration page, configure the following.



Option	Description
PBR Name	Specifies a name for the policy-based route.
Virtual Router	From the Virtual Router drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Type	Specifies the object type that the policy-based route binds to. You can select **Zone**, **Virtual Router**, **Interface** or **No Binding**. • Zone: Click this option button and select a zone from the **Bind To** drop-down list. • Virtual Router: Click this option button and show the virtual router that the policy-based route bind to. • Interface: Click this option button and select a interface from the **Bind To** drop-down list. • No Binding: This policy-based route is no binding.

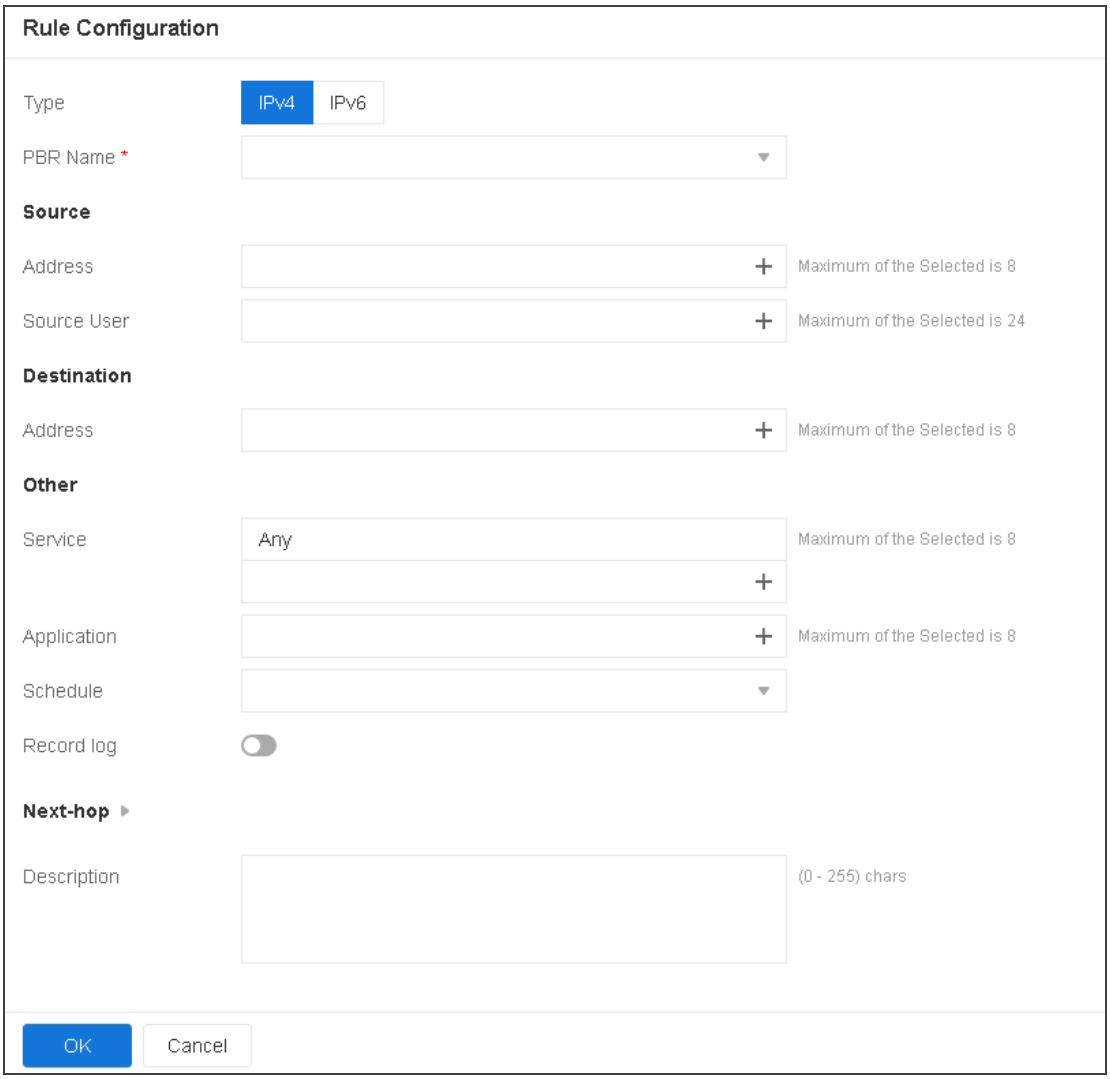
3. Click **OK**.

Creating a Policy-based Route Rule

To create a Policy-based Route rule, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **New**. Select **Rule** from the drop-down list.



Option	Description
PBR Name	Specifies a name of the policy-based route to which the the

Option	Description
	policy-based route rule belongs.
Description (Optional)	Type information about the PBR rule.
Source	
Address	Specifies the source addresses of PBR rule. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close**. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ button to create a new address entry. • You can click ▼ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter

Option	Description
	"10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched.
Source User	Specifies a role, user or user group for the PBR rule. 1. From the **User** drop-down menu, select the AAA server which the users and user groups belongs to. To specify a role, select **Role** from the **AAA Server** drop-down list. 2. Based on different types of AAA server, you can execute one or more actions: search a user/user group/role, expand the user/user group list, enter the name of the user/user group. 3. After selecting users/user groups/roles, click them to add them to the left panes. 4. After adding the desired objects, click the **Close** to complete the user configuration.
Destination	
Address	Specifies the destination addresses of PBR rule. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selec-

Option	Description
	ted type. 3. Click **Add** to add the addresses to the left panes. 4. After adding the desired addresses, click **Close**. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ button to create a new address entry. • You can click ▼ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched.
Other	

Option	Description
Service	Specifies a service or service group. 1. From the **Service** drop-down menu, select a type: Service, Service Group. 2. You can search the desired service/service group, expand the service/service group list. 3. After selecting the desired services/service groups, click them to add them to the left panes. 4. After adding the desired objects, click **Close**. You can also perform other operations: • To add a new service or service group, select **User-defined** from the **Predefined** drop-down listr, and click ⊕ button. • The default service configuration is any. To restore the configuration to this default one, select the **any** check box.
Application	Specifies an application/application group/application filters. 1. From the **Application** drop-down menu, you can search the desired application/application group/application filter, expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click them to add them to

Option	Description
	the left panes. 3. After adding the desired objects, click **Close** to complete the application configuration. You can also perform other operations: • To add a new application group, click **New AppGroup**. • To add a new application filter, click **New AppFilter**. **Note**: Deprecated predefined applications cannot be added.
Schedule	Specifies a schedule when the PBR rule will take effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click **Close** to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Record log	Click the **Enable** button to enable the logging function for PBR rules.

Expand Next-hop, configure the following.

Option	Description
Set Next-hop	To specify the type of next hop, click **IP Address**, **Virtual Router in current Vsys**, **Interface**. • IP Address: Type IP address into the **IP address** text box and specify the weight into the **Weight** text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value.

Option	Description
	• Virtual Router in current Vsys: Select a name from the **Next-Hop Virtual Router** drop-down list and specify the weight into the **Weight** text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value. • Interface: Select an interface from the **Interface** drop-down list and specify the weight into the **Weight** text box. When more than one next hops are available, the traffic will be allocated to the different next hops according to the weight value.
Track Object	Select the track object from the drop-down list or click ⊕ button to create a new track object. See "Track Object" on Page 985.
Weight	Specifies the weight for the next hop. The value range is 1 to 255. The default value is 1. If a PBR rule is configured with multiple next hops, system will distribute the traffic in proportion to the corresponding weight.
Add	Click to add the specified next hop.
Delete	Select next-hop entries from the next hop table and click this button to delete.

Adjusting Priority of a PBR Rule

To adjust priority of a Policy-based Route rule, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.

3. Select the rule you want to adjust priority from the list below, click **Priority**.

In the Priority page, enter values.



Option	Description
Top	Click this option button to move the PBR rule to the top.
Bottom	Click this option button to move the PBR rule to the bottom.
Before ID	Click this option button and type the ID into the box to move the PBR rule to the position before the ID.
After ID	Click this option button and type the ID into the box to move the PBR rule to the position after the ID.

Notes: Each PBR rule is labeled with a unique ID. When traffic flows into a Hillstone device, the device will query for PBR rules by turn, and process the traffic according to the first matched rule. However, the PBR rule ID is not related to the matching sequence during the query. You can move a PBR rule's location up or down at your own choice to adjust the matching sequence accordingly.

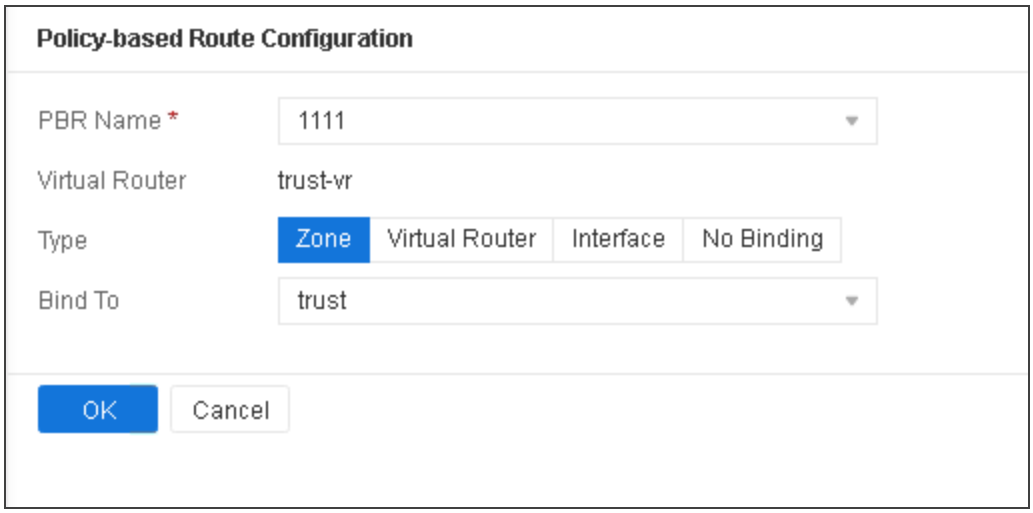
Applying a Policy-based Route

You can apply a policy-based route by binding it to an interface, virtual router or zone.

To apply a policy-based route, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.
3. Click **Bind to**.

   In the Policy-based Route Configuration page, enter values.



Option	Description
PBR Name	Select a route from the PBR name drop-down list.
Virtual Router	From the **Virtual Router** drop-down list, select the Virtual Router for the new route. The default value is "trust-vr".
Type	Specifies the object type that the policy-based route binds to. You can select **Zone**, **Virtual Router**, **Interface** or **No Binding**. • Zone: Click this option button and select a zone from the **Bind To** drop-down list. • Virtual Router: Click this option button and show the virtual router that the policy-based route binds to. • Interface: Click this option button and select a interface

Option	Description
	from the **Bind To** drop-down list. • No Binding: This policy-based route is no binding.

4. Click **OK**.

DNS Redirect

System supports the DNS redirect funtion, which redirects the DNS requests to a specified DNS server. For more information about specifying IP addresses of the DNS server, see Configuring a DNS Server. Currently, the DNS redirect function is mainly used to redirect the video traffic for load balancing. With the policy based route working together, system can redirect the Web video traffic to different links, improving the user experience.

To enable the DNS redirect function, take the following steps:

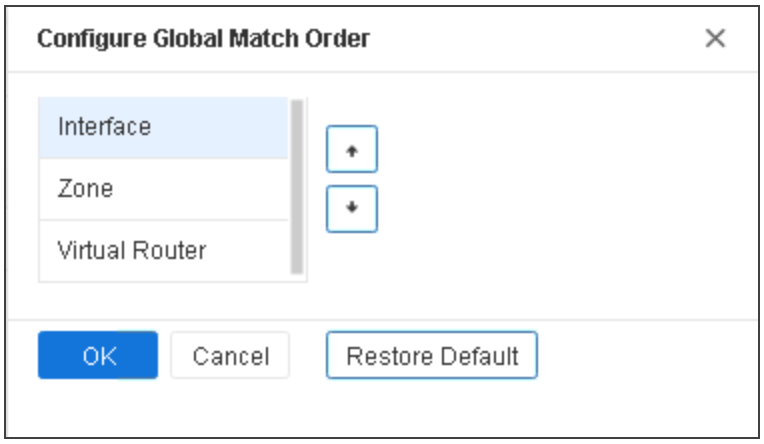
1. Select **Network** > **Routing** > **Policy-based Routing**.
2. Click **Enable DNS Redirect**.

Configuring the Global Match Order

By default, if the PRB rule is bound to both an interface , VRouter and the security zone the interface belongs to, the traffic matching sequence will be: Interface > Zone > VRouter. You can configure the global match order of PBR.

To configure the global match order, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.
2. Click **Config Global Match Order**.



3. Select the items that need to be adjusted, and click  and .
4. To restore the default matching sequence, click **Restore Default**.
5. Click **OK**.

RIP

RIP, Routing Information Protocol, is an internal gateway routing protocol that is designed to exchange routing information between routers. Currently, devices support both RIP versions, i.e., RIP-1 and RIP-2.

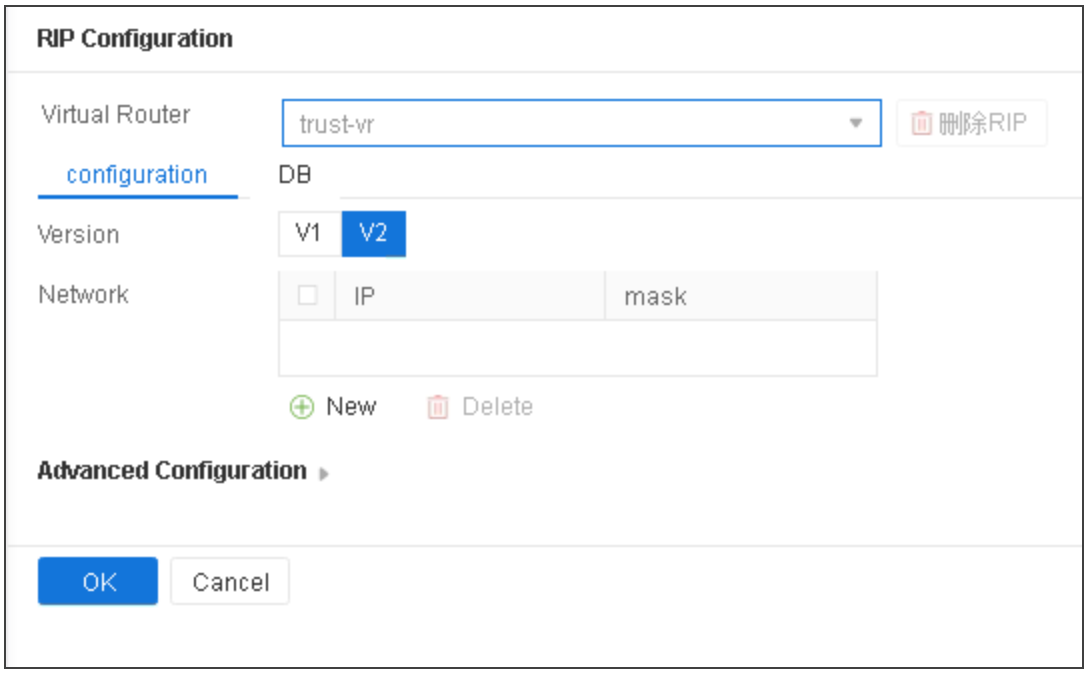
RIP configuration includes basic options, redistribute, Passive IF, neighbor, network and distance. You will also need to configure RIP parameters for different interfaces, including RIP version, split horizon, and authentication mode.

Creating RIP

To create RIP, take the following steps:

1. Select **Network** > **Routing** > **RIP**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.

3. Click **New**.



In the configuration tab, configure the following.

Option	Description
Version	Specifies a RIP version. Hillstone devices support RIP-1 and RIP-2. RIP-1 transmits packets by broadcasting, while RIP-2 transmits packet by multicasting. Select a version from the drop-down list. The default version is RIP-2.
Network	
Network (IP/netmask)	Type the IP address and netmask into the **Network(IP/net-mask)** box.
New	Click **New** to add the network. All the networks that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more networks. To delete a net-work, select the entry you want to delete from the list, and click

Option	Description
	Delete.

Click Advanced Configuration, configure the following.

Option	Description
Metric	Specifies a default metric. The value range is 1 to 15. If no value is specified, the value of 1 will be used. RIP measures the distance to the destination network by hops. This distance is known as metric. The metric from a router to a directly connected network is 1, increment is 1 for every additional router between them. The max metric is 15, and the network with metric larger than 15 is not reachable. The default metric will take effect when the route is redistributed.
Distance	Specifies a default distance. The value range is 1 to 255. If no value is specified, the value of 120 will be used.
Default-info originate	Specifies if the default route will be redistributed to other routers with RIP enabled. By default RIP will not redistribute the default route. Click the **Enable** button to redistribute the default route.
Update interval	Specifies an interval in which all RIP routes will be sent to all the neighbors. The value range is 0 to 16777215 seconds. The default value is 30.
Invalid time	If a route has not been updated for the invalid time, its metric will be set to 16, indicating an unreachable route. The value range is 1 to 16777215 seconds. The default value is 180.
Hold-down	If the metric becomes larger (e.g., from 2 to 4) after a route has

Option	Description
time	been updated, the route will be assigned with a holddown time. During the holddown time, the route will not accept any update. The value range is 1 to 16777215 seconds. The default value is 180.
Flush time	System will keep on sending the unreachable routes (metric set to 16) to other routers during the flush time. If the route still has not been updated after the end of flush time, it will be deleted from the RIP information database. The value range is 1 to 16777215 seconds. The default value is 240.
Redistribute	
Protocol	Select a protocol type for the route from the **Protocol** drop-down list. The type can be Connected, Static, IS-IS, OSPF or BGP.
New	Click **New** to add the Redistribute route entry. All the entries that have been added will be displayed in the Redistribute Route list below.
Delete	Repeat the above steps to add more Redistribute route entries. To delete a Redistribute route entry, select the entry you want to delete from the list, and click **Delete**.
Neighbor	
Neighbor IP	Type the neighbor IP into the **Neighbor IP** box.
New	Click **New** to add the neighbor IP. All the neighbor IPs that have been added will be displayed in the list below.

Option	Description
Delete	Repeat the above steps to add more neighbor IPs. To delete a neighbor IP, select the entry you want to delete from the list, and click **Delete**.
Distance	
Distance	Type the distance into the **Distance** box. The priority of the specified distance is higher than than the default distance.
Network (IP/netmask)	Type the IP prefix and netmask into the **Network(IP/netmask)** box.
New	Click **New** to add the distance. All the distances that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more distances. To delete a distance, select the entry you want to delete from the list, and click **Delete**.

Click **Interface Configuration**, configure the following.

Option	Description
Edit	Select the check box of an interface from the Interface page, and click **Edit** to open the Interface Configuration page.

In the DB tab, view the database of the RIP route.

All the route entries that can reach target network are stored in the database.

4. Click **OK**.

Notes: Configuration for RIP on Hillstone device's interfaces includes: RIP version, split horizon and authentication mode. For more information on how to configure RIP on an interface, see "Configuring an Interface" on Page 158.

OSPF

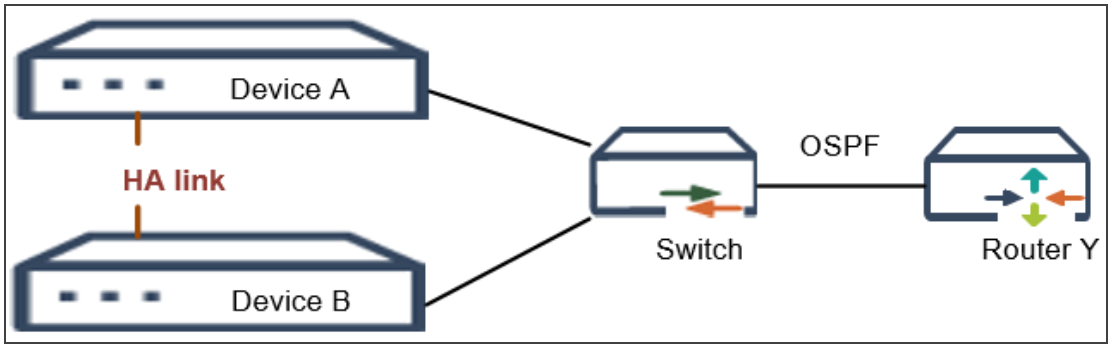
OSPF, the abbreviation for Open Shortest Path First, is an internal gateway protocol based on link state developed by IETF. The current version of OSPF is version 2 (RFC2328). OSPF is applicable to networks of any size. Its quick convergence feature can send update message immediately after the network topology has changed, and its algorithm assures it will not generate routing loops. OSFP also have the following characteristics:

- Area division: divides the network of autonomous system into areas to facilitate management, thereby reducing the protocol’s CPU and memory utilization, and improving performance.
- Classless routing: allows the use of variable length subnet mask.
- ECMP: improves the utilization of multiple routes.
- Multicasting: reduces the impact on non-OSPF devices.
- Verification: interface-based packet verification ensures the security of the routing calculation.

Note: Autonomous system is a router and network group under the control of a management institution. All routers within an autonomous system must run the same routing protocol.

OSPF GR

Graceful Restart (GR) is also called Non-Stop Forwarding (NSF). In a network environment running the OSPF protocol, OSPF GR can ensure that network traffic is not interrupted during HA switchover.



As shown in the picture above, devices A and B form an HA Active-Passive (A/P) mode. During HA switchover, the OSPF neighborhood between the new primary device and the neighboring device Router Y will be disconnected and reestablished, causing route flapping and service interruption. After configuring the OSPF GR function, when performing HA switchover, the new primary device enters the GR Restarter state and sends a Grace LSA to neighbor Router Y, announcing information such as the GR interval, GR reason, and interface address. After receiving the Grace LSA, Router Y enters the GR Helper state and maintains neighborhood with the new primary device during the GR interval, assisting the new primary device in completing the GR and ensuring uninterrupted data forwarding.

Basic Concepts of OSPF GR:

- GR Restarter: GR Restarter is the device applying Graceful Restart during BGP restart or the switchover between backup and primary devices.
- GR Helper: Neighbor of the GR Restarter, a device that assists the GR Restarter in the GR process.
- Grace LSA: Grace LSA is a type of Type-9 LSA of Opaque LSA used to support the OSPF GR feature. It is generated during High Availability (HA) switchover and advertises information such as GR interval, GR reason, and interface address to OSPF neighbors.



Notes:

- OSPF GR feature supports HA Active-Passive (A/P) mode and SCM HA, but does not support HA Peer mode.
- Devices in the following scenarios can act as GR Restarter, while devices in other scenarios can only act as GR Helper:
  - The newly elected primary device after HA switchover
  - Devices (X6150/X6180/X7180/X9180/X10800/K9180) that perform SCM HA switchover.



- OSPF GR feature will not take effect if the HA connection between the primary and backup devices is disconnected.

Creating OSPF

To create OSPF, take the following steps:

1. Select **Network** > **Routing** > **OSPF**.
2. From the **Virtual Router** drop-down list, select the Virtual Router for the new route.
3. Click **New**.

Option	Description
Process ID	Enter the OSPF process ID. The default value is 1. The value ranges from 1 to 65535. Each OSPF process is individual, and has its own link state database and the related OSPF routing table. Each VRouter supports up to 4 OSPF processes and multiple OSPF processes maintain a routing table together. When specifying the OSPF process ID, note the following matters: • When running multiple OSPF processes in a VRouter, the network advertised in interfaces in each OSPF process cannot be same. • When route entries with the same prefix exist in multiple OSPF processes, the system will compare the administrative distance of each route entry and the route entry with the lower administrative distance will

Option	Description
	be added to the VRouter's routing table. If their AD is the same, the route entry that was first discovered will be added to the routing table. • If the OSPF route entries are redistributed to other routing protocols, the routing information of process 1 will be redistributed by default. If this process does not exist, the routing information of OSPF will not be redistributed.
Router ID	Enter the Router ID used by OSPF protocol. Each router running OSPF protocol should be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole OSPF domain, represented in the form of an IP address.
HA Synchronization	Click the **Enable** button to enable HA synchronization. The OSPF configuration of the master and backup will be synchronized.
Enable Opaque Capability	Turn on the switch to enable Opaque LSA capability. Opaque LSA is an extended universal mechanism for OSPF. It includes Type-9 LSA, Type-10 LSA, and Type-11 LSA. Opaque LSA supports OSPF GR functionality through the Grace LSA in Type-9 LSA. **Note**: Opaque LSA capability should be enabled before using the OSPF GR feature.
Enable GR	Turn on the switch to enable the GR function of the GR

Option	Description
	Restarter. You can also specify GR interval in the **GR Interval** part. GR interval refers to the timeout time of GR. During the GR interval, the GR Helper will maintain neighborhood with the GR Restarter. After the GR interval expires, regardless of whether the GR is complete or not, the GR Helper will exit the GR Helper state. The value range is from 1 to 1,800 seconds. The default value is 120 seconds. It is recommended to extend the GR interval when there are many neighbors.
Enable GR Helper	Turn on the switch to enable the GR Helper function. You can also turn on the switch of Enable GR Helper Strict LSA Check. After configuring GR Helper Strick LSA Check, when the GR Helper device detects a change in LSA, it will exit the GR Helper state.
Network	Configure the network interface that enables OSPF and add the network to the specified area. Click **New**, and enter the network address, network mask and area ID. • Network Address: Enter the IP address of network interface that enables OSPF protocol. • Network Mask: Enter the mask of IP address. • Area ID: Enter the area ID the network will be added to, in form of a 32-bit digital number, or an IP address.
Redistribute Configuration	

Option	Description
Static	Click the **Enable** button to redistribute the static route protocol into the OSPF route and advertise the route to OSPF neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
Connected	Click the **Enable** button to redistribute the connected route protocol into the OSPF route and advertise the route to OSPF neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
RIP	Click the **Enable** button to redistribute the RIP route protocol into the OSPF route and advertise the route to OSPF neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the

Option	Description
	Route Map Configuration panel. For more information about how to configure a route map, see "Route Map" on Page 431.
OSPF	Click the **Enable** button to specify the process ID, redistribute other OSPF processes into this process, and advertise the processes to OSPF neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
ISIS	Click the **Enable** button to redistribute the ISIS route protocol into the OSPF route and advertise the route to OSPF neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
BGP	Click the **Enable** button to redistribute the BGP route protocol into the OSPF route and advertise the route to OSPF neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing

Option	Description
	information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
VPN	Click the **Enable** button to redistribute the VPN route into the OSPF route and advertise the route to OSPF neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
DOMAIN	Click the **Enable** button to redistribute the domain route into the OSPF route and advertise the route to OSPF neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.

4. Click **OK**.

Notes: Configuration for OSPF on Hillstone device's interfaces includes: hello transmission interval, dead time, LSA transmit interval and LSU transmit delay time. For more information on how to configure OSPF on an interface, see "Configuring an Interface" on Page 158.

Viewing the Neighbor Information

To view the neighbor information, take the following steps:

1. Select **Network** > **Routing** > **OSPF**.
2. Select the process ID check box, and the neighbor information will be displayed in the list below.



- Neighbor Router ID: Shows the router ID of OSPF neighbors.
- Priority: Shows the router priority. The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and broadcast the received link information.
- Neighbor State: Shows the OSPF neighbor state. The OSPF neighbor state includes 8 types: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading and Full. The Full state includes Full/DR and Full/BDR.
- Timeout: Shows the neighbor timeout, which is the difference between dead time and hello transmission interval. The unit is second. If the OSPF doesn't receive the Hello packets from neighbor, the neighbor ship cannot be established continually.

- Neighbor IP: Shows the IP address of neighbor router.
- Local Interface: Shows the interface sends the Hello packets to the neighbor router.

Configuring OSPFv3

OSPFv3 is the third version of Open Shortest Path First and mainly provides the support of IPv6. Before configuring OSPFv3, you need to enable IPv6 at **Network** > **Interface** > **New**, and configure an OSPFv3 interface. For how to configure the OSPFv3 interface, refer to **Configuring an Interface**.

The similarities between OSPFv3 and OSPFv2 are as follows:

- Both protocols use 32 bits Router ID and Area ID.
- Both protocols use the Hello packets, DD (database description) packets, LSR (link state request) packets, LSU (link state update) packets, and LSAck (link state acknowledgment) packets.
- Both protocols use the same mechanisms of finding neighbors and establishing adjacencies.
- Both protocols use the same mechanisms of LSA flooding and aging.

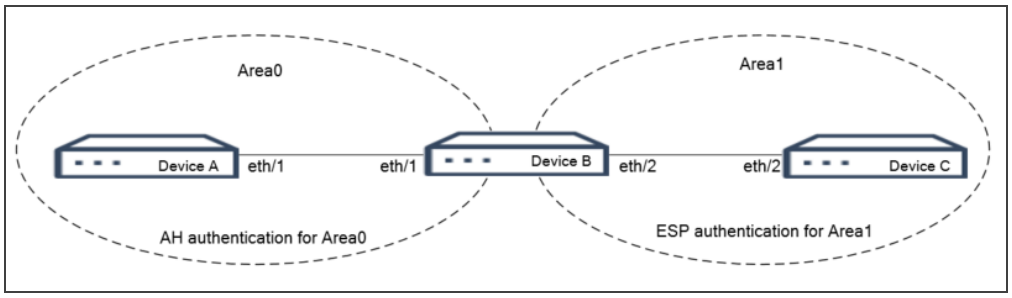
The differences between OSPFv3 and OSPFv2 are as follows:

- OSPFv3 runs on a per-link basis and OSPFv2 is on a per-IP-subnet basis.
- OSPFv3 supports multiple instances per link.
- OSPFv3 identifies neighbors by Router ID, and OSPFv2 identifies neighbors by IP address.

You can configure the OSPFv3 protocol for each VRouter respectively.

OSPFv3 can use IPSec Authentication Header (AH) and IPSec Encapsulating Security Payload (ESP) header capabilities to achieve encryption and authentication between neighbor devices. You can enable encryption and authentication for an OSPFv3 area and on an interface within the OSPFv3 area.

- When you need to protect all OSPFv3 packets in an area, you can enable encryption and authentication for this area. In this case, all devices in this area needs to be configured with the same encryption and authentication policy, including the authentication method, SIP value, authentication algorithm, authentication key, etc.
- When you need to protect OSPFv3 packets of a specified interface within an area, you can enable encryption and authentication on this interface. In this case, the interface of the directly connected neighbor needs to be configured with the same encryption and authentication policy, including the authentication method, SIP value, authentication algorithm, authentication key, etc.



Creating OSPFv3

To create the OSPFv3 process, take the following steps:

1. Select **Network** > **Routing** > **OSPFv3**.
2. Select a VR from the **Virtual Router** drop-down list.
3. Click **New** to open the **OSPFv3 Configuration** page.

Option	Description
Process ID	Enter the OSPFv3 process ID. The default value is 1. The value ranges from 1 to 65535. Each OSPFv3 process is individual, and has its own link state database and the related

Option	Description
	OSPFv3 routing table. Each VRouter supports up to 4 OSPFv3 processes and multiple OSPFv3 processes maintain a routing table together. When specifying the OSPFv3 process ID, note the following matters: • When running multiple OSPFv3 processes in a VRouter, the network advertised in interfaces in each OSPFv3 process cannot be same. • When route entries with the same prefix exist in multiple OSPFv3 processes, the system will compare the administrative distance of each route entry and the route entry with the lower administrative distance will be added to the VRouter's routing table. If their AD is the same, the route entry that was first discovered will be added to the routing table. • If the OSPFv3 route entries are redistributed to other routing protocols, the routing information of process 1 will be redistributed by default. If this process does not exist, the routing information of OSPFv3 will not be redistributed.
Router ID	Specifies the router ID of the router running the OSPFv3. The router ID is the unique identifier of an router in the OSPFv3 domain. The router ID should be in the format of IP address.

Option	Description
HA Synchronization	Click the **Enable** button to enable HA synchronization. The OSPFv3 configuration of the master and backup will be synchronized.
IPv6 Redistribute Configuration	
Static	Click the **Enable** button to redistribute the static route protocol into the OSPFv3 route and advertise the route to OSPFv3 neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
Connected	Click the **Enable** button to redistribute the connected route protocol into the OSPFv3 route and advertise the route to OSPFv3 neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
RIPng	Click the **Enable** button to redistribute the RIPng route protocol into the OSPFv3 route and advertise the route to

Option	Description
	OSPFv3 neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
OSPFv3	Click the **Enable** button to specify the process ID, redistribute other OSPFv3 processes into this process, and advertise the processes to OSPFv3 neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
ISISv6	Click the **Enable** button to redistribute the ISISv6 route protocol into the OSPFv3 route and advertise the route to OSPFv3 neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about

Option	Description
	how to configure a route map, see "Route Map" on Page 431.
BGP+	Click the **Enable** button to redistribute the BGP+ route protocol into the OSPFv3 route and advertise the route to OSPFv3 neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431.
Cryptographic Authentication: Click New to enable encryption and authentication for the OSPFv3 area	
Area ID	Enter the area ID of OSPFv3, which can be a 32-bit digital number, or an IP address.
Authentication Method	Select an authentication method for the OSPFv3 area from the drop-down list. Valid values: AH and ESP. Note: AH authentication does not support data encryption. In other words, you cannot configure the Encryption Algorithm and Encryption Key parameters.
Security Parameter Index	Enter the Security Parameter Index (SPI) value. Valid values: 256 to 4294967295. The receiver authenticates received packets by using the SPI value.
Authentication Algorithm	Select an authentication algorithm in the OSPFv3 area from the drop-down list. Valid values: MD5 and SHA1.
Authentication	Enter the authentication key in the hexadecimal string format

Option	Description
Key	in the OSPFv3 area.
Encryption Algorithm	If the Authentication Method parameter is set to ESP, you need to specify the encryption algorithm, which can be "-", "DES", "3DES", "AES-128", "AES-192", or "AES-256". "-" indicates that no encryption algorithm is specified and ESP provides only the authentication function.
Encryption Key	After you specify the encryption algorithm, you need to enter a corresponding encryption key in the hexadecimal string format. **Note:** If the Encryption Algorithm parameter is set to "-", you do not need to configure an encryption key.
Virtual Link Configuration	
Area ID	Virtual link is used to connect the discontinuous backbone areas, so that they can maintain logical continuity. Specifies an area ID that requires virtual link, in form of a 32-bit digital number, or an IP address.
Virtual Link To Peer ABR Router ID	Virtual link always connect two area border routers. You need to configure the router ID of the area border routers respect-ively.

4. Click **OK** to save the configurations and the created OSPFv3 process will be displayed in the list.

5. Expand **Interface Configuration**, configure the following.

Option	Description
Edit	Select the check box of an interface from the Interface page, and click **Edit** to open the Interface Configuration page.
Interface Area Configuration	Configure the area and instance where the OSPFv3 interface belongs to. • **Interface**: Specifies the interface running OSPFv3. • **Area ID**: Specifies the area ID that the interface belongs to. The area ID is in form of a 32-bit digital number, or an IP address. • **Instance ID**: Specifies the instance ID that the interface belongs to. To establish the neighbor relationship, interfaces must belong to the same instance. The value ranges from 0 to 255. The default value is 0. • **Interface Timer**: There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets. • Hello Transmission Interval: Specifies the interval for sending Hello packets for an interface. The value range is 1 to 65535

Option	Description
	seconds. The default value is 10. If the OSPFv3 interface chooses the point-to-multipoint network type, the default value is 30. • Dead Time: Specifies the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets). If the OSPFv3 interface chooses the point-to-multipoint network type, the default value is 120.If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. • LSA Transmit Interval: Specifies the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5. • LSU Transmit Delay Time: Specifies the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1.

Option	Description
	• **Priority**: Specifies the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the designated router (The designated router will receive the link information of all the other routers in the network, and broadcast the received link information). If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected. • **Network Type**: Specifies the network type of an interface. The network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast. • **Link Cost**: The value range is 1 to 65535. By default, the HA synchronization function is enabled, and the link cost will be synchronized to the backup device. Clear the check box to disable the synchronization function, and the system will stop synchronizing. • **Passive**: Click the button to enable the interface as passive interface. The interface which receives

Option	Description

	data only but not send is known as a passive interface.
	• **MTU-Ignore**: Click the button to ignore the MTU check. OSPFv3 uses DBD packets to check whether the interface MTU set is matched or not between the neighbors. If the MTU set is not matched, the neighbors cannot establish the adjacency. You can modify the MTU set to solve this issue. For the interfaces whose MTU set cannot be modified, you can ignore the MTU check.
	• **Cryptographic Authentication**: Turn on the switch to enable the Cryptographic Authentication function in the interface within the OSPFv3 area. By default, this function is disabled.
	  • Authentication Method: Specifies the authentication method of the OSPFv3 interface. Valid values: AH, ESP, AH NULL, and ESP NULL. AH NULL indicates that AH authentication is disabled for the interface. ESP NULL indicates that ESP authentication is disabled for the interface.
	  • Security Parameter Index: Specifies the Security Parameter Index (SPI) value. Valid values: 256 to 4294967295. The receiver

Option	Description
	authenticates received packets by using the SPI value. • Authentication Algorithm: Select an authentication algorithm of the OSPFv3 interface from the drop-down list. Valid values: MD5 and SHA1. • Authentication Key: Enter the authentication key in the hexadecimal string format of the OSPFv3 interface. • Encryption Algorithm: If the Authentication Method parameter is set to ESP, you need to specify the encryption algorithm, which can be "-", "DES", "3DES", "AES-128", "AES-192", or "AES-256". "-" indicates that no encryption algorithm is specified and ESP provides only the authentication function. • Encryption Key: After you specify the encryption algorithm, you need to enter a corresponding encryption key in the hexadecimal string format. **Note:** If the Encryption Algorithm parameter is set to "-", you do not need to configure an encryption key.



Notes:

Take note of the following rules for the Cryptographic Authentication function of the OSPFv3 route:

- If the Cryptographic Authentication function is enabled for an area and is disabled on all interfaces within this area, the encryption and authentication policy of the area is applied to these interfaces.
- If the Cryptographic Authentication function is enabled for both an interface and the area where the interface belongs and the authentication method of the interface is neither AH NULL nor ESP NULL, the encryption and authentication policy of the interface takes effect.
- If the Cryptographic Authentication function is enabled for the area where the interface belongs and the authentication types of the interface and the area are different and the authentication method of the interface is NULL, the encryption and authentication policy of the area is applied to the interface. For example, if the area where the interface belongs is configured with AH authentication and the interface is configured with ESP NULL, the encryption and authentication policy of this area is applied to this interface.
- If the Cryptographic Authentication function is enabled for the area where the interface belongs and the authentication types of the interface and the area are the same but the authentication method of the interface is NULL, no encryption and no authentication is performed on packets on this interface. For example, if the area where the interface belongs is configured with ESP authentication and the interface is configured with ESP NULL, no encryption and no authentication is performed on packets on this interface.

- Both the interface and the area where the interface belongs can be configured with only one authentication method.

Viewing Neighbor Information

To view the neighbor information of the created OSPFv3 process, take the following steps:

1. Select **Network** > **Routing** > **OSPFv3**.
2. Select an OSPFv3 process and the neighbor information will be displayed below.



- Neighbor Router ID: Displays the ID of neighbor router.
- Priority: Displays the router priority. The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and send the received link information.
- Link Local Address: Displays the Link-local of the neighbor router interface.
- Neighbor State: Displays the OSPFv3 neighbor state. The OSPFv3 neighbor state includes 8 types: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading and Full. The Full state includes Full/DR and Full/BDR.
- Timeout: Displays the neighbor timeout, which is the difference between dead time and hello transmission interval. The unit is second. If the OSPFv3 doesn't receive the Hello packets from neighbor, the neighbor ship cannot be established continually.

- Local Interface: Displays the interface sending the Hello packets to the neighbor router.

Configuring BGP

BGP, the abbreviation for Border Gateway Protocol, is a routing that is used to exchange dynamic routing information among the autonomous systems. Autonomous system means the router and network group under the control of a management institute. When BGP runs within the autonomous system, it is called IBGP (Internal Border Gateway Protocol); when BGP runs between the autonomous systems, it is called EBGP (External Border Gateway Protocol).

BGP GR

GR (Graceful Restart) is also called Non-Stop Forwarding (NSF).

The BGP GR ensures that the forwarding layer can continue to forward data during the switchover between backup and primary devices or device restart. Meanwhile, the operation of the forwarding layer is not affected by the re-establishment of neighbor relations and the routing computation of the control layer. In this scenario, BGP GR can help the system have less single point of failure, and reduce the influence of route flapping on the network during the switchover between backup and primary devices. Therefore, the network is more reliable and can avoid the influence of traffic interruption on users' important services.

Basic Concepts of BGP GR

- End-of-RIB marker: End-of RIB marker is a BGP Update message with no reachable Network Layer Reachability Information (NLRI) and its withdrawn NLRI is empty. When the current device receives the End-of-RIB marker from its peer, it indicates that this peer has sent all updates needing to be notified.
- Graceful Restart Capability: Graceful Restart Capability is a new BGP capability to better support GR functionality. It is advertised by the BGP with the Open message when a BGP connection is established. Graceful Restart Capability can indicate that the current device can

preserve its forwarding state during BGP restart, and generate the End-of-RIB marker upon the completion of its initial updates.

- GR Restarter: GR Restarter is the device applying Graceful Restart during BGP restart or the switchover between backup and primary devices.
- GR Helper: GR Helper is the neighbor of GR Restarter, and is the device with GR Capability to assist GR Restarter in the Graceful Restart.

A device can be a GR Restarter or a GR Helper. Whether to become a GR Restarter or a GR Helper is determined according to the actual role the device plays in the procedures of BGP GR.

Take device HA as an example. The working procedures of BGP GR are as follows:

1. In device HA, the new primary device works as the GR Restarter and re-establishes the BGP connection with the GR Helper.
2. The GR Helper disconnects its BGP neighborhood with the previous primary device and marks the BGP routes learned from the previous primary device as stale. But the GR Helper still forwards data messages via these routes and enables the Graceful-Restart Stale-Path-Time. To configure the Graceful-Restart Stale-Path-Time, use the **graceful-restart stale-path-time** *time* command.
3. If the GR Restarter successfully establishes the BGP session with the GR Helper within the notified Graceful-Restart Restart-Time, they become neighbors and will exchange routing information. If the GR Restarter cannot establish a BGP neighborhood with the GR Helper within the notified Graceful-Restart Restart-Time, the GR Helper will delete routes related to the GR Starter immediately. To configure Graceful-Restart Restart-Time, use the **graceful-restart restart-time** *time* command.
4. GR Helper sends updates after becoming a neighbor of the GR Restarter and generates an End-of-RIB marker upon the completion of the updates. Even if the GR Helper does not have updates to be notified, it is required to send the End-of-RIB marker.

5. GR Restarter starts to select the optimum path after receiving the End-of-RIB markers from its peers. If GR Restarter does not receive all the necessary End-of-RIB markers, it will start to select the optimum path after the configured Graceful-Restart Wait-For-Rib-Time expires. To configure the Graceful-Restart Wait-For-Rib-Time, use the **graceful-restart wait-for-rib-time** *time* command.

6. After the selection of the optimum path, GR Restarter updates the RIB, then generates updates of the BGP route and sends the updates to its BGP neighbors. Whether there are updates or not, GR Restarter should notify the End-of-RIB marker.

7. After receiving the route updates, GR Helper removes the stale markers of relative routes. GR Helper will remove routes still with stale markers after receiving the End-of-RIB marker sent by the GR Restarter.

8. If routing information exchange is not completed within the Graceful-Restart Stale-Path-Time, GR Restarter is forced to quit GR and then GR Restarter updates RIB according to the learned BGP route information and deletes invalid RIB.



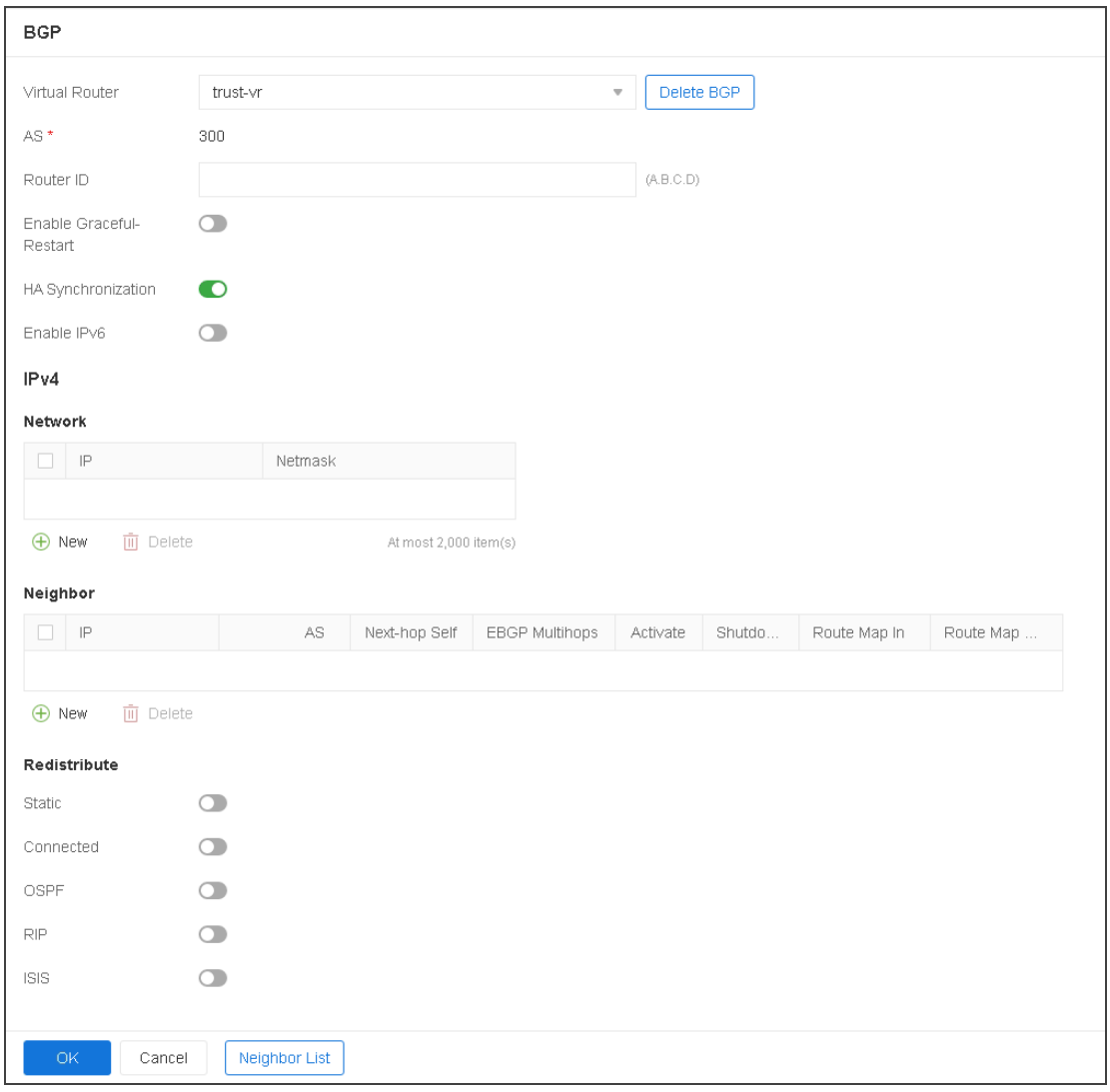
Notes:

- BGP GR cannot be applied in HA peer mode.
- Only when devices in the below scenarios can they work as the GR Restarter. Otherwise, they work as the GR Helper.
  - The newly elected primary device after HA switching;
  - Devices with SCM HA function, such as X6150/X6180/X7180/X9180/X10800/K9180.
- BGP GR does not work if HA between primary and backup devices dis-connects.

Basic

To configure a basic process, take the following steps:

1. Select **Network** > **Routing** > **BGP**
2. Select a VR from the **Virtual Router** drop-down list. The default VR is "trust-vr".
3. In this page, enter the basic information of BGP.



4. Configure the options as follows:

Option	Description
AS	Specifies the number of Autonomous System, ranging from 1 to 4294967295.
Enable Graceful-Restart	Click the **Enable** button. • Graceful-Restart Restart-Time: Specifies the longest time for a peer to wait for a BGP session to be re-established. The time range from 1 to 3600 seconds. The default Graceful-Restart Restart-Time is 120 seconds. • Graceful-Restart Stale-Path-Time: Specifies the longest time to retain the stale routes of the restarted peers. The time range from 1 to 3600 seconds. The default Graceful-Restart Stale-Path-Time is 360 seconds. • Graceful-Restart Wait-For-Rib-Time: Specifies the longest time for the GR Restarter to wait for the End-of-RIB markers from the neighbors. The time range from 1 to 3600 seconds. The default Graceful-Restart Wait-For-Rib-Time is 180 seconds.
Router ID	Specifies the router ID of the router running the BGP. The router ID is the unique identifier of an router in the BGP domain. The router ID should be in the format of IP address.
Enable IPv6	Click the **Enable** button to support the format of IPv6 address.
HA sync	Click this button to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device;

Option	Description
	not clicking this button disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
Enable IPv6	Click the **Enable** button to expand the IPv6 configuration items.
IPv4	
Network	You can add the specified network in the local routing table to the BGP routing table, and remove the specified network from the list. Then the network will be learned by the neighbor router configured later. • Add: Click the ⊕ button, and specify the IPv4 address and netmask. When IPv6 is enabled, you can specify the IPv6 address and prefix. • Delete: If you want to delete the specified network, click the 🗑 button.
Neighbor	You can add neighbor routers to exchange routing information with the specified router, or delete the specified router from the list. You can add at most 8 neighbor routers. • Add: To add a neighbor router, click the ⊕ button and enter the information as follows. • **IP**: Enter the IP address of the specified neighbor

Option	Description
	router. • **AS**: Specify the AS number of the neighbor router, ranging from 1 to 4294967295. • **Next-hop Self**: For a neighbor router of the EBGP, if the next-hop address of the IBGP of the neighbor router cannot be reached, you should enable the next-hop as self. • **EBGP Multihops**: For BGP running between different AS (i.e., EBGP), if the specified router and its neighbor router are not directly connected, you need to configure EBGP multi-hops, ranging from 0 to 255. • **Activate**: You can activate the BGP connection between the configured neighbor router and the current device. By default, the function is enabled. • **Shutdown**: You can shutdown the neighbor router in the list. When it's shut down, all sessions with the neighbor router will be cut and all router information will be cleared. By default, the function is disabled. • **Route Map In**: Filter routes that are accepted by the neighbor router by using the route map. Only the acceptance of specific routing information can

Option	Description
	be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • **Route Map Out**: Filter routes that are advertised by the neighbor router by using the route map. Only the advertisement of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • Delete: To delete the specified neighbor router, click the  button.
Redistribute	When IPv4 is supported, the following routing protocols can be introduced and redistributed. • **Static**: Select the check box to redistribute the static route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific

Option	Description
	routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • **Connected**: Select the check box to redistribute the connected route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • **OSPF**: Select the check box to redistribute the OSPF route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For

Option	Description
	more information about how to configure a route map, see "Route Map" on Page 431. • **RIP**: Select the check box to redistribute the RIP route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • **IS-IS**: Select the check box to redistribute the IS-IS route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. When IPv6 is supported, the following routing protocols can be redistributed and advertised.

Option	Description
	• **Static**: Select the check box to introduce the static route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • **Connected**: Select the check box to introduce the connected route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • **OSPFv3**: Select the check box to introduce the OSPFv3 route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific

Option	Description
	routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • **RIPng**: Select the check box to introduce the RIPng route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For more information about how to configure a route map, see "Route Map" on Page 431. • **ISISv6**: Select the check box to introduce the ISISv6 route protocol into the BGP route and advertise the route to BGP neighbors. You can also use route maps to filter routing information. Only the redistribution of specific routing information can be allowed or denied. To use a route map, select a configured route map from the **Route Map** drop-down list. Alternatively, click "+" to create a route map in the **Route Map Configuration** panel. For

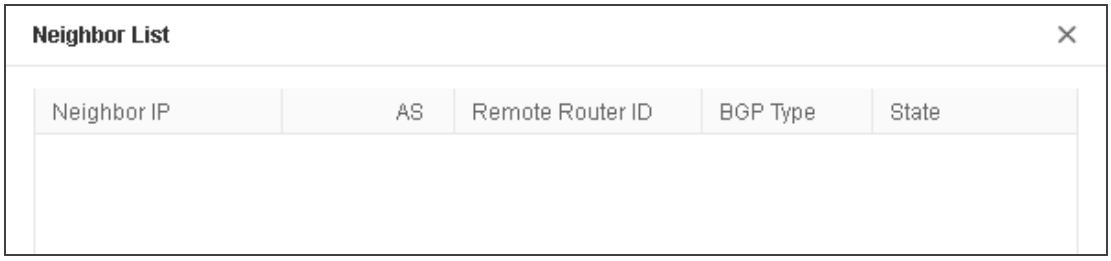
Option	Description
	more information about how to configure a route map, see "Route Map" on Page 431.

5. Click **OK** to save the configurations. The newly-created nwighbor router will be displayed in the list.

Neighbor List

To view the created neighbor router, take the following steps:

1. Select **Network** > **Routing** > **BGP**.
2. In the **Neighbor List** page, view the information of neighbor routers.



- **Neighbor IP**: Displays the IP address of the neighbor router.
- **AS**: Displays the autonomous system number of the neighbor router.
- **Remote Router ID**: When the neighbor router is connected with the peer router, the router ID of the peer router will be displayed.
- **BGP Type**: Displays the running type of BGP. When BGP runs between different AS, it displays as EBGP; when BGP runs within an AS, it displays as IBGP.
- **State**: Displays the status of connection between the neighbor router and its router, including Idle, Connect, Active, OpenSent, OpenConfirm and Established.

Delete BGP

To delete the BGP process, take the following steps:

1. Select **Network** > **Routing** > **BGP**.
2. Click the **Delete BGP** button, and all BGP configurations will be deleted.

Route Object

The following route objects are provided:

- "Route Map" on Page 431
- "Access List Route" on Page 440
- "AS Path Access List" on Page 444
- "Community List" on Page 446

Route Map

The OSPF protocol, OSPFv3 protocol, BGP protocol, and IPv6 BGP protocol allow you to import routing information from other routing protocols and advertise the information. By default, the system imports all the routing information. You can filter the routing information imported from other routing protocols by referencing a route map. The route map mainly consists of two parts: matching rules and actions (permit or deny) for the matched routing information. If imported routing information hits any matching rule, the system will take the configuration action, i.e., permit or deny the imported routing information.



Notes:

- If the action is set to Permit, the system will only permit the matched routing information and deny all the unmatched routing information.



- If the action is set to Deny, the system will deny the matched routing information, but still permit all the unmatched routing information.

To configure a route map and filter the imported routing information, take the following steps:

1. Create a route map and add matching rules to the route map. Matching rules are differentiated by IDs. The smaller the ID is, the higher the matching priority will be. By default if the routing information hits any matching rule, the system will not continue to match the subsequent rules; if no matching rule is hit, the system will take the Deny action.

2. Add matching conditions to the matching rules. The matching condition can be the AS path, community, next-hop interface, destination address, next-hop IP address, metric, or tag of the imported routing information. The matching conditions that can be configured vary based on imported routing protocols. One matching rule may contain multiple matching conditions, and the relation between these conditions is AND, i.e., in order to hit a matching rule, the routing information needs to meet all the matching conditions in the rule.

Match Condition	Support of different imported routing protocols for match conditions			
	OSPF	OSPFv3	BGP	IPv6 BGP
AS Path	x	x	Yes	Yes
Community List	x	x	Yes	Yes
Next Hop Interface	Yes	Yes	x	x
IPv4 Destination Address	Yes	x	Yes	x
IPv6 Destination Address	x	Yes	x	Yes
IPv4 Next Hop	Yes	x	Yes	x
IPv6 Next Hop	x	x	x	Yes

Match Condition	Support of different imported routing protocols for match conditions			
	OSPF	OSPFv3	BGP	IPv6 BGP
Metric	Yes	x	Yes	Yes
Tag	Yes	x	Yes	x

Note: "x" indicates that the match condition is not supported.

3. If the match condition is the destination address or next-hop IP address, also configure a route access-list that will be referenced. For more information about route access-list, see "Access List Route" on Page 440.

4. If needed, require the system to continue to match another rule after the routing information hits a matching rule.

5. If needed, modify partial attributes of the imported routing information before redistribution. The routing attributes that can be modified vary based on imported routing protocols.

Routing Attribute	Support of different routing protocols for modifying routing attributes			
	OSPF	OSPFv3	BGP	IPv6 BGP
AS Path	x	x	Yes	Yes
Community List	x	x	Yes	Yes
Community	x	x	Yes	Yes
Next Hop Interface	x	x	x	x
IPv4 Destination Address	x	x	x	x
IPv6 Destination Address	x	x	x	x

Routing Attribute	Support of different routing protocols for modifying routing attributes			
	OSPF	OSPFv3	BGP	IPv6 BGP
IPv4 Next Hop	x	x	Yes	x
IPv6 Next Hop	x	x	x	Yes
Metric	Yes	Yes	Yes	Yes
Metric Type	Yes	Yes	x	x
Origin	x	x	Yes	Yes
Tag	Yes	x	x	x
Local Preference	x	x	Yes	Yes

Note: "x" indicates that the routing attribute is not supported.

Configuring a Route Map

To create a route map, take the following steps:

1. Select **Network** > **Routing** > **Route Object**.
2. In the **Route Map** tab, click **New** to enter the **Route Map Configuration** page.
3. In the **Name** field, enter the name of the route map.
4. In the Rule section, click **New**.

Option	Description
Sequence Number	Specifies the sequence number for the match rule in the route map.
Operation	Specifies the action for the matched routing information. Valid values: **Permit** and **Deny**.
Match Conditions	
Match Tag	Specifies the tag that matches the route. If the configured tag value of the route matches the tag value in the static route, the match is considered successful.
Match Metric	Specifies the metric that matches the route.
Match IPv4 Destination Address	Specifies the IPv4 destination address that matches the route. To do this, select a configured IPv4 access list route from the drop-down list. Alternatively, click "+" from the drop-down list and create an access list route in the **IPv4 Access List Route Configuration** panel. If the destination address of the route belongs to allowed addresses in the access list route, the match is considered successful. For more information about the access

Option	Description
	list route configuration, see "Access List Route" on Page 440.
Match IPv6 Destination Address	Specifies the IPv6 destination address that matches the route. This parameter is available only when the system version is IPv6. To do this, select a configured IPv6 access list route from the drop-down list. Alternatively, click "+" from the drop-down list and create an access list route in the **IPv6 Access List Route Configuration** panel. If the destination address of the route belongs to allowed addresses in the access list route, the match is considered successful. For more information about the access list route configuration, see "Access List Route" on Page 440.
Match IPv4 Next Hop	Specifies the IPv4 next-hop address that matches the route. To do this, select a configured IPv4 access list route from the drop-down list. Alternatively, click "+" from the drop-down list and create an access list route in the **IPv4 Access List Route Configuration** panel. If the next-hop address of the route belongs to allowed addresses in the access list route, the match is considered successful. For more information about the access list route configuration, see "Access List Route" on Page 440.
Match IPv6 Next Hop	Specifies the IPv6 next-hop address that matches the route. This parameter is available only when the system version is IPv6. To do this, select a configured IPv6 access list route from the drop-down list. Alternatively, click "+" from the drop-down list and create an access list route in the IPv6 Access List Route Configuration panel. If the next-hop address of the route belongs to allowed addresses in the access list route, the match is con-

Option	Description
	sidered successful. For more information about the access list route configuration, see "Access List Route" on Page 440.
Next Hop Interface	Specifies the next-hop interface that matches the route. To do this, select an existing interface from the drop-down list. Alternatively, click "+" from the drop-down list, select an interface type, and then create an interface. For more information about the interface configuration, see "Configuring an Interface" on Page 158.
Match AS Path List	Specifies the AS path that matches the route. To do this, select a configured AS path access list from the drop-down list. Alternatively, click "+" from the drop-down list and create an AS path access list in the **AS Path Access List Configuration** panel. If the AS path of the route matches the AS path allowed in the access list, the match is considered successful. For more information about the AS path access list configuration, see "AS Path Access List" on Page 444.
Match Community List	Specifies the community attribute that matches the route. To do this, select a configured community attribute list name or number from the drop-down list. Alternatively, click "+" from the drop-down list, create a community attribute list in the **Community List Configuration** panel. You can also select **Accurate** to perform exact match on community attribute. For more information about the community attribute list configuration, see "Community List" on Page 446.

Option	Description
Set the condition	
Set Tag	Modifies the tag value of the route to be imported.
Set Metric	Modifies the metric value of the route to be imported.
Set Metric Type	Modifies the metric type of the external routing. **Null** indicates that the metric type is not modified; **Type-1** indicates that the metric type is modified to Type1; **Type-2** indicates that the metric type is modified to Type2.
Set Origin	Specifies the origin of the route to be imported. **Null** indicates that the origin of the imported route is not modified; **IGP** indicates that the imported route is modified to be originated within AS; **EGP** indicates that the imported route is modified to be obtained by using EGP; **Incomplete** indicates that the imported route is modified to be obtained by using other methods.
Set Local Preference	Modifies the local preference of the route to be imported.
Set IPv4 Next Hop	Modifies the IPv4 next-hop address of the route to be imported.
Set IPv6 Next Hop	Modifies the IPv6 next-hop address of the route to be imported. This parameter is available only when the system version is IPv6.
Delete Community List	Deletes the community attribute of the route to be imported. To do this, select a configured community attribute list name or number from the drop-down list. Alternatively, click "+" from the drop-down list, create a community attribute list in the **Community List Configuration** panel. For more information about the

Option	Description
	community attribute list configuration, see "Community List" on Page 446.
Set Community	Modifies the community attribute of the route to be imported. You can enter multiple community attributes in the field at the same time. Separate communities with spaces. One or more of the following communities can be entered: internet, local-AS, no-advertise, no-export, and the number 1 to 4294967295. You can enter a maximum of 8 communities. You can also enter an "additive" to the end of the communities, which indicates that new communities are added to the community of the route to be imported. Example: internet local-AS no-advertise no-export 88 99 51 21 additive. This indicates that the "internet", "local-AS", "no-advertise", "no-export", "88", "99", "51", and "21" attributes are added to the community attributes of the route to be imported.
Set AS Path Prepend	Appends a new AS path to the AS path of the route to be imported. To do this, click **New** and enter an AS path in the field.
Options	
Match Other Rules	By default, if the imported routing information hits a route matching rule, the system no longer matches subsequent rules. You can specify that the system continues to match other rules after a rule is hit. This achieves fine-grained control. To do this, select **Yes** and specify the sequence number of the rule that you want to match in the **Next Sequence** field. This sequence number needs to be greater than the sequence number of the current rule. If this parameter is not specified, the

Option	Description
	system continues to match the next rule after the current rule is successfully matched.

5. Click **OK**. The newly created route matching rule is displayed in the rule list.
6. If required, repeat steps 4 and 5 to configure multiple route matching rules.
7. Click **OK**. The newly created route map is displayed in the route map list.

Notes: If you only create a route map without configuring any route matching rule in the map, the system assumes that the imported routing information is successfully matched by default.

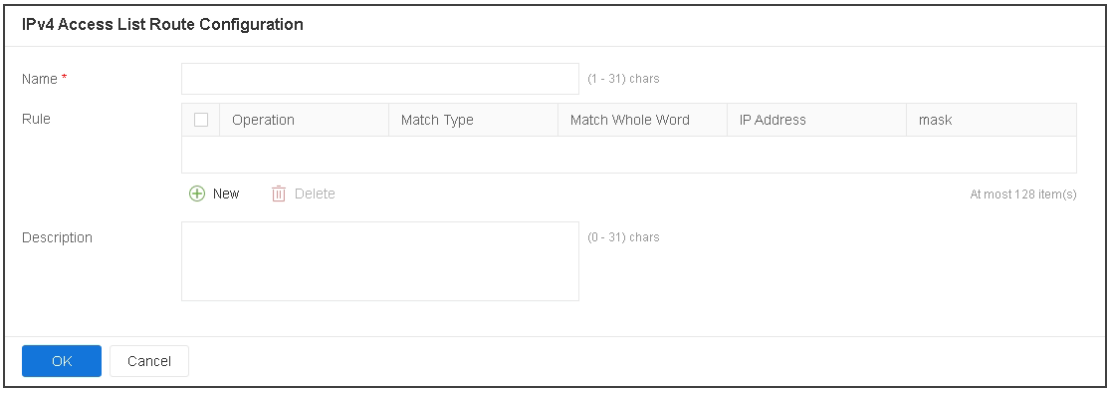
Access List Route

The matching of destination address and next-hop address in route matching rules is achieved by referencing the access list route. The access list route consists of two parts: IP address matching rule and the corresponding operation (allow or deny) to be performed upon successful match. If the destination address or next-hop address matches the specified IP address, the system proceeds to execute the specified action. An access list route can contain multiple IP address matching rules. The system matches the rules in the order of the time when they were added. Once a rule is hit, the matching process immediately ends. If the matching fails, the system performs the deny operation.

Configuring an Access List Route

To configure an IPv4 access list route, take the following steps:

1. Select **Network** > **Routing** > **Route Object**.
2. In the **Access List Route** tab, click **IPv4**.
3. Click **New**.



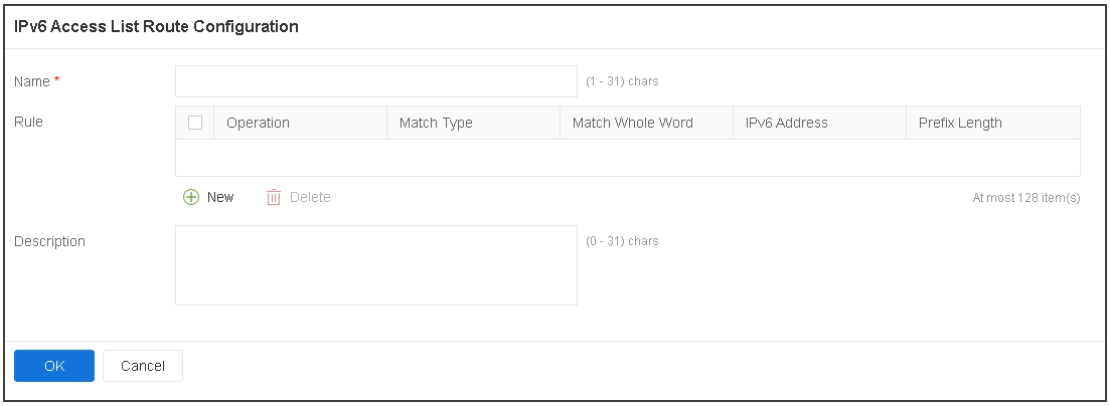
Option	Description
Name	Specifies the name of the access list route.
Rule	Specifies the IP address matching rule and the operation performed after the rule is matched. To do this, click **New** and specify the operation, match type, whether to match whole word, IP address, and subnet mask in the fields. • Operation: Select an operation to be performed on the matched IPv4 address from the drop-down list. • Match Type: Select a match type from the drop-down list. "Any" indicates that any IPv4 address can be matched. • Match Whole Word: Select whether to perform exact

Option	Description
	match on the IPv4 prefix from the drop-down list. • IP Address: Enter the IPv4 address that you want to match. • mask: Enter the subnet mask of the IPv4 address. The subnet mask can be written in one of the two methods. For example, if the IP address that you want to match is "1.1.1.0/24", you can enter "24" or "255.255.255.0" in the field.
Description	Enter a description for the access list route.

4. Click **OK**.

The IPv6 access list route can be configured only when the system version is IPv6. To configure the IPv6 access list route, take the following steps:

1. Select **Network** > **Routing** > **Routing Object**.
2. In the **Access List Route** tab, click **IPv6**.
3. Click **New**.



Option	Description
Name	Specifies the name of the access list route.
Rule	Specifies the IP address matching rule and the operation performed after the rule is matched. To do this, click **New** and specify the operation, match type, whether to match whole word, IPv6 prefix, and prefix length in the fields. • Operation: Select an operation to be performed on the matched IPv6 address from the drop-down list. • Match Type: Select a match type from the drop-down list. "Any" indicates that any IPv6 address can be matched. • Match Whole Word: Select whether to perform exact match on the IPv6 prefix (does not include the prefix length) from the drop-down list. • IPv6 Address: Enter the IPv6 prefix that you want to match. • Prefix Length: Enter the prefix length of the IPv6 address.
Description	Enter a description for the access list route.

4. Click **OK**.

AS Path Access List

The AS path is the sequence of AS numbers that route traverses before reaching the destination network. Before advertising a route to anther AS, BGP adds the local AS number into the AS_ PATH attribute.

You can implement route filtering based on the AS path access list, which consists of two parts: a regular expression and the corresponding operation (permit or deny) to be performed upon successful matches. If the regular expression matches the AS path of the route, the system proceeds to execute the specified operation. Otherwise, the system performs the deny operation. You can configure at most 64 AS path access lists and each AS path access list can have at most 8 regular expressions configured.

Configuring an AS Path Access List

To configure an AS path access list, take the following steps:

1. Select **Network** > **Routing** > **Route Object**.
2. In the **AS Path Access List** tab, click **New**.



Option	Description
List Number	Specifies the AS path access list number.
Rule	Specifies the regular expression and the operation performed after the regular expression is matched. To do this, click **New** and specify the following options: • Operation: Select an operation that you wan to perform on the matched route from the drop-down list. • Regular Expression: Enter a regular expression, which is used to match the AS path. The system supports the PCRE regex syntax.

3. Click **OK**.

Community List

A BGP community is a group of routes with the same characteristics, independent of their associated IP subnets and ASs. Besides custom community attributes, the system supports the following well-known BGP community attributes:

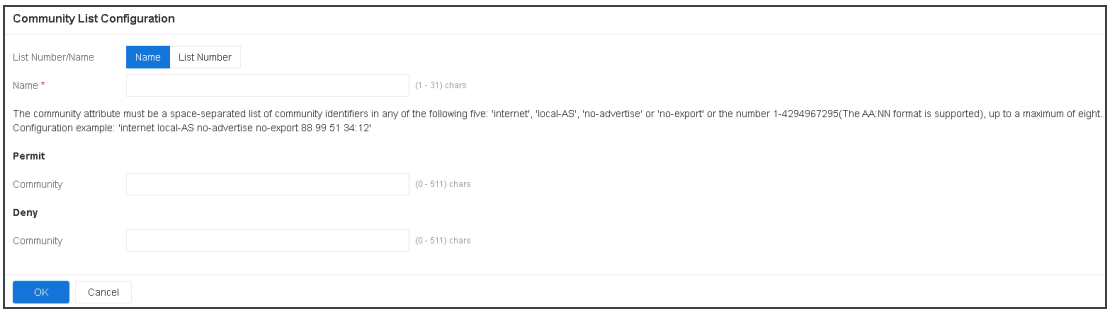
- No-export: Routes with this community attribute cannot be advertised to peers that are outside the AS.
- No-adverties: A route with this attribute cannot be advertised to any other BGP peers.
- Local-as: Routes with this community attribute can be advertised to other peers only in the local AS.
- Internet: By default, all routes belong to the Internet community. A route with this attribute can be advertised to all BGP peers.

Configuring a Community List

To configure a community list, take the following steps:

1. Select **Network** > **Routing** > **Route Object**.

2. In the **Community List** tab, click **New**.



Option	Description
List Number/Name	Specifies the name or list number of the community list.
Permit	Sets the operation to be performed on the matched route to Permit. You can enter multiple community attributes in the field at the same time. Separate communities with spaces. One or more of the following communities can be entered: internet, local-AS, no-advertise, no-export, and the number 1 to 4294967295 (The AA:NN format is supported). You can enter a maximum of 8 communities. You can also enter an "additive" to the end of the communities, which indicates that new communities are added to the community of the route to be imported. Example: internet local-AS no-advertise no-export 88 99 51 21 additive. This indicates that the "internet", "local-AS", "no-advertise", "no-export", "88", "99", "51", and

Option	Description
	"21" attributes are added to the community attributes of the route to be imported.
Deny	Sets the operation to be performed on the matched route to Deny. You can enter multiple community attributes in the field at the same time. Separate communities with spaces. One or more of the following communities can be entered: internet, local-AS, no-advertise, no-export, and the number 1 to 4294967295 (The AA:NN format is supported). You can enter a maximum of 8 communities. You can also enter an "additive" to the end of the communities, which indicates that new communities are added to the community of the route to be imported. Example: internet local-AS no-advertise no-export 88 99 51 21 additive. This indicates that the "internet", "local-AS", "no-advertise", "no-export", "88", "99", "51", and "21" attributes are added to the community attributes of the route to be imported.

3. Click **OK**.

Configuring Protocol Independent Multicast (PIM)

The Protocol Independent Multicast (PIM) indicates that static route or any unicast routing protocol, such as RIP, OSPF, IS-IS, or BGP, can provide the routing information for IP multicast. Multicast routing is not dependent on the unicast routing protocols, as long as the multicast routing tables are generated by the unicast routing protocols.

According to different mechanisms, PIM is divided into the following two modes:

- PIM-DM (Protocol Independent Multicast-Dense Mode): applies to small-scale networks in which receivers are densely distributed.
- PIM-SM (Protocol Independent Multicast-Sparse Mode): applies to large-scale networks in which receivers are sparsely distributed.

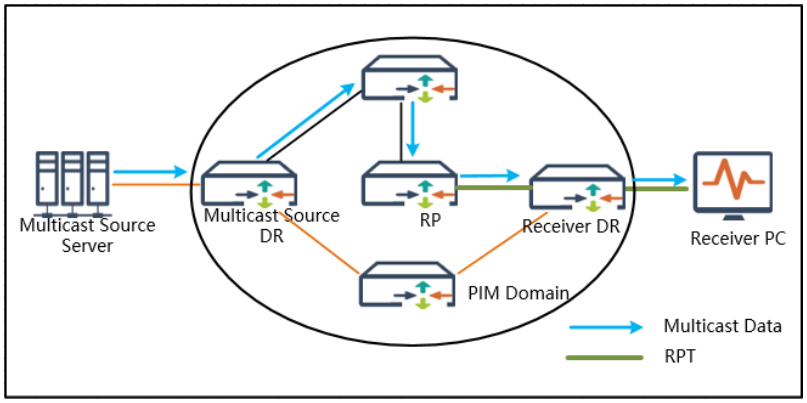
Currently, the system only supports the PIM-SM mode.

Basic Principles of PIM-SM

PIM-SM (Protocol Independent Multicast-Sparse Mode) can resolve P2MP data transmission problems in a large-scale network where users are sparsely distributed.

PIM-SM assumes that no host wants to receive multicast data. The PIM device forwards multicast data to the host only when a host requests multicast data explicitly.

PIM-SM sends the multicast information to the PIM device in the PIM domain through the configured RP (Rendezvous Point) and BSR (BootStrap Router), and then an RPT (Rendezvous Point Tree) will be built. Multicast data can be forwarded to the receiver along the RPT through the RP.



The key concepts of PIM-SM are as follows:

- **PIM Domain**: A network formed by PIM devices.
- **DR (Designated Router)**: There are two types of DR in a PIM network.
    - **Multicast source DR**: A PIM device that is directly connected to the multicast source in a PIM-SM domain and is responsible for sending Register messages to the RP.
    - **Receiver DR**: A PIM device that is directly connected to group members (receiver hosts) and is responsible for forwarding multicast data to the group members.
- **RP (Rendezvous Point)**: An RP is the core of a PIM-SM network, which can be divided into the static RP and dynamic RP. An RPT is a shared tree with an RP as the root and members of multicast group as the leaves in a PIM-SM network.
- **BSR (BootStrap Router)**: A BSR of a PIM-SM network, which is responsible for collecting and distributing RP information.
- **RPT (Rendezvous Point Tree)**: An RPT is a multicast distribution tree (MDT) with an RP as the root and members of multicast group as the leaves.
- **SPT (Shortest Path Tree)**: A shortest path tree (SPT) is a multicast distribution tree (MDT) with the multicast source as the root and members of multicast group as leaves.

PIM-SSM

PIM-SM needs to maintain Rendezvous Points (RPs) to transmit multicast data. If receivers know the exact location of a multicast source and want to request multicast data directly from the multicast source, Protocol Independent Multicast-Source-Specific Multicast (PIM-SSM) can enable receiver hosts to rapidly join multicast groups by maintaining relationship between hosts and routers through IGMPv3. A shortest path tree (SPT) is set up between the multicast source and group members without maintaining an RP. The multicast data will be forwarded to receivers along the SPT.

Configuring PIM

The configuration of PIM includes basic configuration and the configuration of PIM-SM on different interfaces.



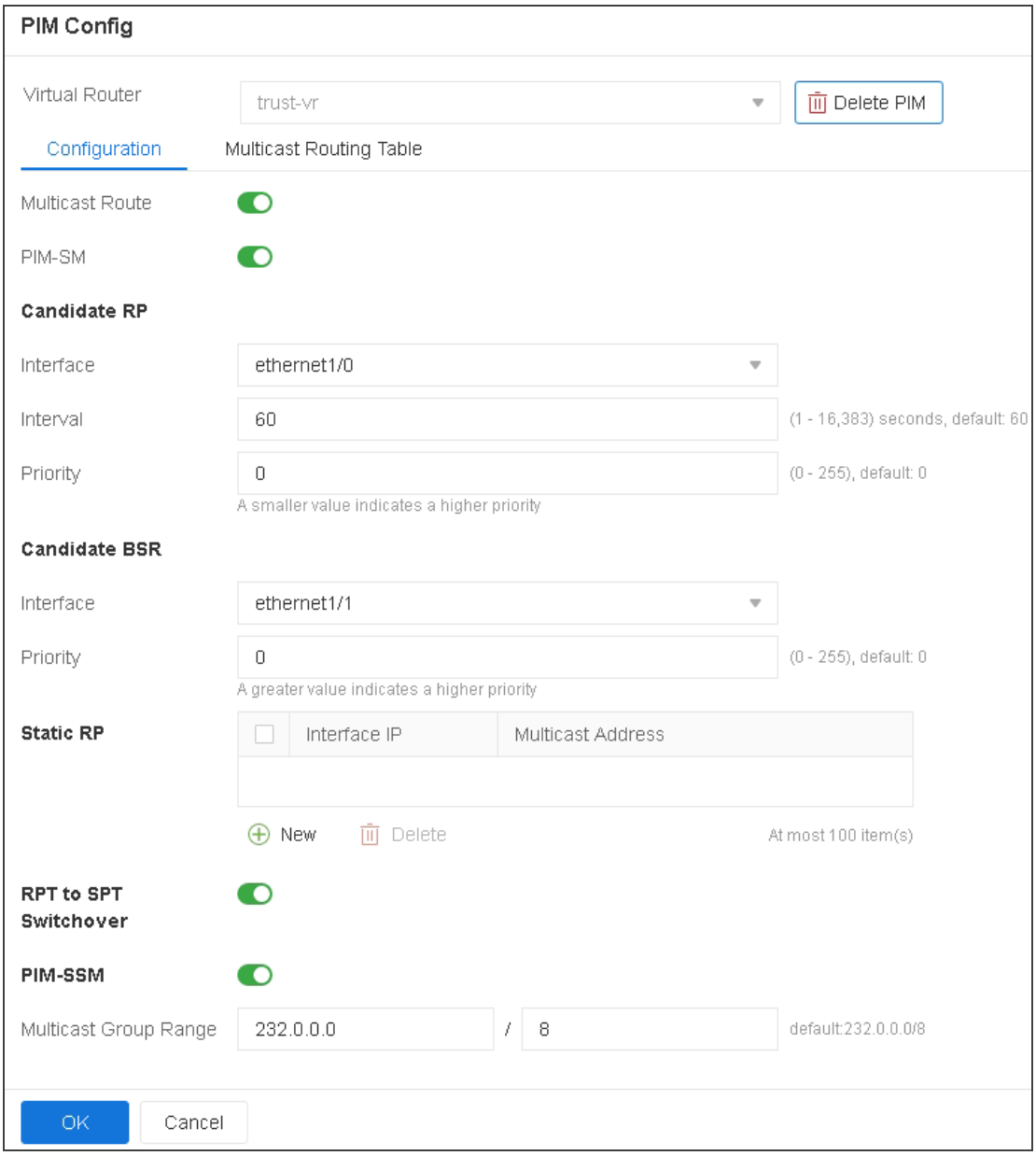
Notes:

- The PIM-SM function cannot be configured with the static multicast routing function or the IGMP Proxy function at the same time.
- PIM-SSM function is on the basis of the PIM-SM function. Configure PIM-SM mode before configuring the PIM-SSM.
- In HA environment, PIM-SSM only supports Active-Passive (A/P) mode.
- The PIM-SM function can only be enabled on the Layer 3 interface.

To configure PIM, take the following steps:

1. Select **Network** > **Routing** > **PIM**
2. Select a virtual router where the new PIM belongs from the **Virtual Router** drop-down list.

3. Select the **Configuration** tab to specify basic parameters.



On the Configuration tab, configure the following options.

Option	Description
Multicast Route	Turn on the switch button to enable global multicast routing.

Option	Description
PIM-SM	Turn on the switch button to enable PIM-SM.
Candidate RP	Select PIM devices in the PIM-SM domain to configure them as the candidate RP (Rendezvous Point). RP will be elected from the candidates. Candidate BSR should be configured at the same time and BSR will be elected from the candidate BSR (BootStrap Router). BSR is responsible for collecting and distributing RP information in the network. Candidate RP includes the following configuration: • Interface: Select the interface where the candidate RP resides from the drop-down list. The interface must be enabled with PIM-SM. • Interval: Specifies the interval for sending candidate RP messages. The range is 1 to 16,383 seconds. The default value is 60 seconds. • Priority: Specifies the priority. The smaller the value is, the higher the priority will be. In the RP election, the candidate RP with a higher priority will be elected as the RP. The range is 0 to 255 and the default priority is 0. **Notes:** When configuring a candidate RP, you do not need to specify a multicast address. The default multicast address is 224.0.0.0/4.
Candidate BSR	In a PIM-SM domain, you need to configure one or more candidate BSRs. BSR will be automatically generated among can-

Option	Description
	didate BSRs. The BSR will collect and distribute the RP information. Candidate BSR includes the following configuration: • Interface: Select the interface where the candidate BSR resides from the drop-down list. The interface must be enabled with PIM-SM • Priority: Specifies the priority. The larger the value is, the higher the priority will be. If there is only one candidate BSR in the PIM-SM domain, it will become the BSR. If there are multiple candidate BSRs, the candidate BSR with the higher priority will be elected as the BSR. The range is 0 to 255 and the default priority is 0.  **Notes:** When a dynamic RP is used, the candidate BSR must be configured and at least one candidate BSR must be configured in the PIM-SM domain.
Static RP	When there's only one Rendezvous Point (RP) in the network, you're suggested to configure a static RP rather than a dynamic RP to save the bandwidth occupied by frequent message exchange between the Candidate RP and the BSR. In the PIM-SM domain, the static RP configured on all the devices should be the same. Click **New**. Enter the IP address of the interface where the static RP resides in the **Interface IP** textbox and the multicast address in the **Multicast Address** textbox.
RPT to SPT	Click the switch button to enable RPT to SPT Switchover. Since

Option	Description
Switchover	the RPT (Rendezvous Point Tree) in the PIM-SM domain may not be the shortest path, when the multicast data traffic becomes too high, the RP may become the fault point. To solve the problem, by default, the RPT can be switched to the SPT (Shortest Path Tree). After the switchover, the multicast data can be sent directly from the multicast source to the receiver along the SPT. You can switch RPT to SPT as needed.
PIM-SSM	By default, PIM-SSM is disabled. Click the switch button to enable PIM-SSM and specify the address range of PIM-SSM multicast group in the **Multicast Group Range** textbox. Ensure that the address range of PIM-SSM group configured on all PIM devices in the network are consistent. By default, the address range of PIM-SSM is 232.0.0.0/8.

4. Click **OK**.
5. To delete configured PIM, select a virtual router from the **Virtual Router** drop-down list. Click Delete PIM to delete PIM configuration in this VR

To configure PIM-SM on interfaces, take the following steps:

1. Select **Network** > **Routing** > **PIM**.
2. Click **Interface Configuration** in the upper-right corner.
3. Double-click the interface or select the check box before the interface and click **Edit**.

Option	Description
Interface	Displays the name of the interface.

Option	Description
PIM-SM	Turn on the switch button to enable PIM-SM.
DR Priority	Specifies the priority of DR. The larger the value is , the higher the priority will be. The default value is 1. The value range is 0 to 4,294,967,294. The priority of the DR (Designated Router) is used to determine which router to use as the designated router (DR). All routers in the PIM-SM domain can be specified as DR and the router with higher priority will be selected. If the priority is the same, the one with a larger IP address will be selected.
Hello Interval	With PIM-SM enabled, the interface periodically sends Hello packets. You can specify the interval for sending Hello packets on the interface as needed. The value range is 1 to 65,535 seconds. The default value is 30 seconds.
IGMP Query Interval	Specifies the interval for sending IGMP general query messages. The range is 1 to 18,000 seconds, and the default value is 60 seconds. The network where the receiver host is located may connect to multiple multicast routers. These multicast routers then elect a router as the querier automatically to maintain IGMP group membership of the interface. After the PIM-SM function is enabled for the interface, the querier will send IGMP general query messages to learn about the entry and exit of multicast group members.
IGMP Querier Timeout	Specifies the timeout value for IGMP general query. The range is 30 to 300 seconds, and the default value is 120 seconds.

Option	Description
	If the multicast router in the network does not receive IGMP general query messages within the specified timeout period, multicast routers will elect a querier again.
IGMP Query Max Response Time	Specifies the maximum response time for IGMP general query. The range is 1 to 25 seconds, and the default value is 10 seconds. You can specify the maximum response time after the receiver host receives the general query message. After the querier sends the IGMP general query message twice and no response from the receiver host within the specified maximum response time, the system will delete this receiver in the multicast routing table.
Non-direct Multicast Source	Specifies the non-direct multicast source address. The system cannot establish the neighbor relationship with a multicast source as the muticast source DR across different network segments, and the muticast source DR will discard multicast packets whose network segment is different from the ingress interface. Therefore, you can configure the non-direct multicast source address to ensure that the multicast source DR and multicast source multicast across network segments when unicast routing of the multicast source is reachable for all PIM devices within the multicast domain. Click **New** and configure the multicast source address and subnet mask of non-direct multicast source. You can configure at most 10 non-direct multicast source entries. **Note**: Only root-VSYS supports to configure the multicast

Option	Description
	source address of non-direct multicast source.
Interface joins Multicast Groups	Configures the IGMP Join-group on the interface. This allows the interface of the system to join the multicast group and receive data traffic from the multicast group. You can configure at most 100 multicast groups. • IGMPv2: Select "IGMPv2" and configure the multicast group address. This way, the interface will join the specified multicast group over IGMPv2. • IGMPv3: Select "IGMPv3" and configure the multicast group address and multicast source address. This way, the interface will join the specified multicast group over IGMPv3. **Note**: To use the MSR function, you need to configure the IGMP Join-group function on the Vif interface.
Multicast Service Reflection	The MSR function supports to process multicast data forwarded to the Vif interface by converting the source address and multicast group address of the original multicast stream into a new multicast stream. When multicast traffic matches the ingress interface and pre-reflection destination IP address in the MSR entry, it can be converted to the post-reflection destination IP address and source IP address in the MSR entry. You can configure at most 100 MSR entries. To do this, click **New** and configure the following parameters: • Ingress Interface: Select the ingress interface of the ori-

Option	Description
	ginal multicast stream from the drop-down list. • Destination IP (Before Reflection): Specifies the multicast group address of the original multicast stream. • Destination IP (After Reflection): Specifies the post-reflection multicast group address. • mask (After Reflection): Specifies the post-reflection subnet mask of the multicast group address. • Source IP (After Reflection): Specifies the post-reflection multicast source address, which needs to be in the same network segment as the IP address of the Vif interface. Note: • Only root VSYS supports the MSR function. • When you use the MSR function, if unicast route performs route advertisement learning combined with the OSPF protocol, the OSPF network type on the Vif interface needs to be set to **point-to-point**. This allows the neighbor device to learn non-host routes. For more information about how to configure OSPF on the interface, see Configuring OSPF.

4. Click **OK**.

Viewing PIM Routing Information

To view the multicast routing table, take the following steps:

1. Select **Network** > **Routing** > **PIM**.
2. Select a virtual router from the **Virtual Router** drop-down list.
3. Select the **Multicast Routing Table** tab to view the source address, multicast address, ingress interface, and egress interface of the multicast routing.

Configuring Protocol Independent Multicast (PIMv6)

PIMv6 is used to transfer multicast data in IPv6 network environment. PIMv6 indicates that IPv6 static route or any IPv6 unicast routing protocol, such as RIP, OSPFv3, IPv6 IS-IS, can provide the routing information for IP multicast. Multicast routing is not dependent on the unicast routing protocols, as long as the multicast routing tables are generated by the unicast routing protocols.

PIMv6 shares the same mechanism as that of PIM. PIMv6 only supports IPv6 PIM-SM mode. Main differences between PIMv6 and PIM are:

- Using different protocols to manage members of the multicast group. PIM uses IGMP while PIMv6 uses MLD.
- PIM supports PIM-SSM while PIMv6 does not.

Multicast Listener Discovery (MLD)

Multicast Listener Discovery (MLD) is a protocol that manages IPv6 multicast members. The MLD protocol sets up and maintains memberships between IPv6 hosts and their directly connected multicast routers by exchanging MLD messages between them.

MLD has two versions: MLDv1 defined in RFC2710 and MLDv2 defined in RFC3810.



Notes: Currently, the system only supports MLDv1.

MLDv1

MLDv1 implements IPv6 multicast listener management based on the query and response mechanism.

MLDv1 defines the following messages:

- General Query: A querier sends General Query messages to all hosts and routers on the shared network to discover which multicast groups have members on the shared network.
- Multicast Address Specific Query: A querier sends Multicast Address Specific Query messages to members in a specified multicast group on the shared network segment to check whether the group has members.
- Multicast Listener Report: Hosts send Multicast Listener Report messages to a querier to request to join a multicast group or respond to General Query messages.
- Multicast Listener Done: A host sends a Multicast Listener Done message to notify the querier on the network that it has left a group.

Based on MLDv1, MLDv2 allows hosts to specify whether to accept messages from specific multicast source.

Configuring PIMv6

The configuration of PIMv6 includes basic configuration and the configuration of IPv6 PIM-SM on different interfaces.



Notes:

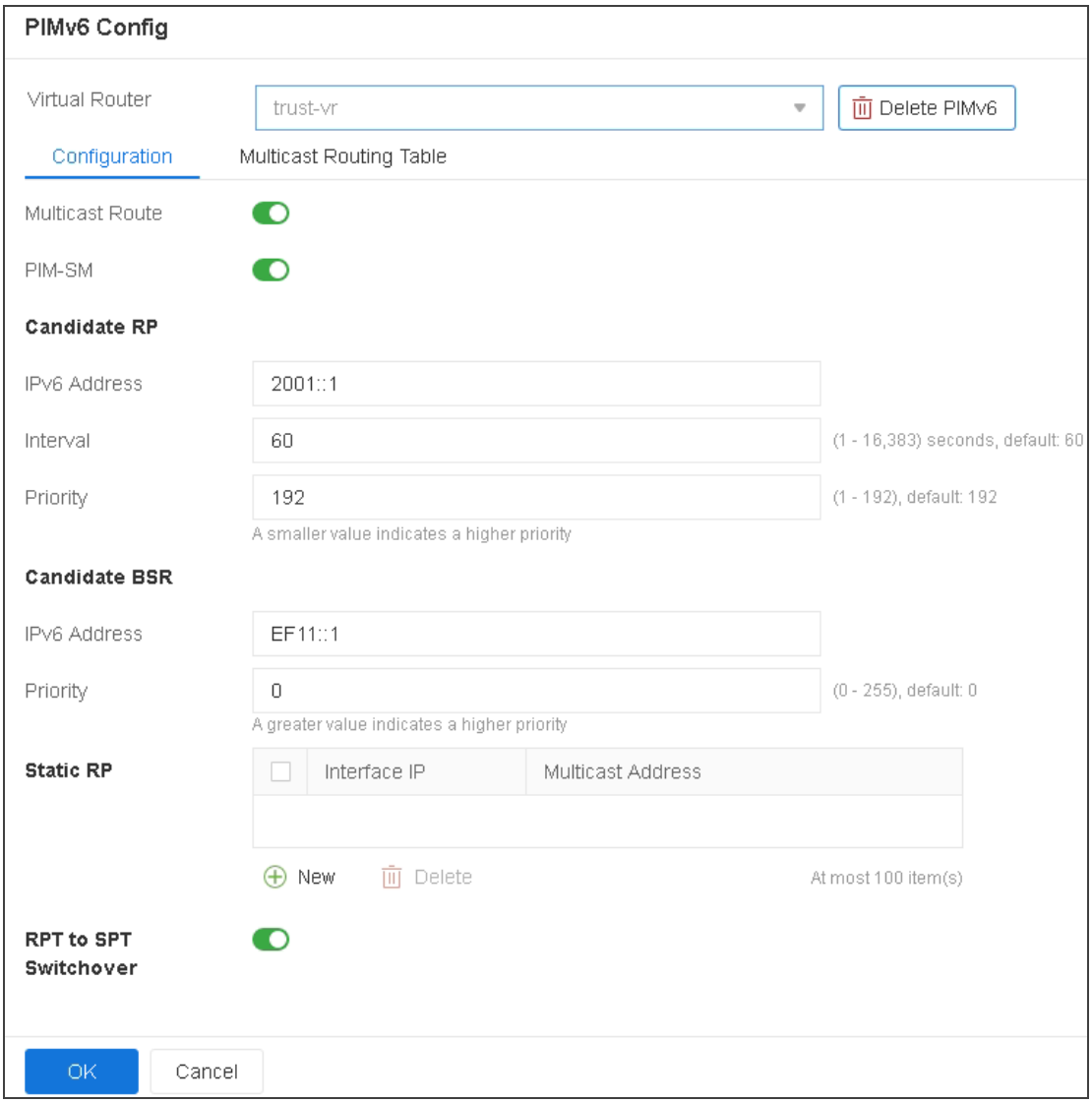
- To configure PIMv6, the current system version should be IPv6.
- The IPv6 PIM-SM function cannot be configured with the IPv6 static multicast routing function at the same time.
- IPv6 PIM-SM function can only be enabled on the Layer 3 interface.

To configure PIMv6, take the following steps:

1. Select **Network** > **Routing** > **PIMv6**.

2. Select a virtual router where the new PIMv6 belongs from the **Virtual Router** drop-down list.

3. Select the **Configuration** tab to specify basic parameters.



Option	Description
Multicast Route	Turn on the switch button to enable IPv6 global multicast routing.

Option	Description
PIM-SM	Turn on the switch button to enable IPv6 PIM-SM.
Candidate RP	Select PIM devices in the IPv6 PIM-SM domain to configure them as the candidate RP (Rendezvous Point). RP will be elected from the candidates. Candidate BSR should be configured at the same time and BSR will be elected from the candidate BSR (BootStrap Router). BSR is responsible for collecting and distributing RP information in the network. Candidate RP includes the following configuration: • IPv6 Address: Specifies the IPv6 address of the candidate RP interface. The address cannot be the link-local address. The interface must be enabled with IPv6 PIM-SM. • Interval: Specifies the interval for sending candidate RP messages. The range is 1 to 16,383 seconds. The default value is 60 seconds. • Priority: Specifies the priority. The smaller the value is, the higher the priority will be. In the RP election, the candidate RP with a higher priority will be elected as the RP. The range is 1 to 192 and the default priority is 192. **Notes:** When configuring a candidate RP, you do not need to specify a multicast address. The default multicast address is FF00::/8.
Candidate BSR	In a IPv6 PIM-SM domain, you need to configure one or more candidate BSRs. BSR will be automatically generated amon-

Option	Description
	gcandidate BSRs. The BSR will collect and distribute the RP information. Candidate BSR includes the following configuration: • IPv6 Address: Specifies the IPv6 address of the candidate BSR interface. The address cannot be the link-local address. The interface must be enabled with IPv6 PIM-SM. • Priority: Specifies the priority. The larger the value is, the higher the priority will be. If there is only one candidate BSR in the IPv6 PIM-SM domain, it will become the BSR. If there are multiple candidate BSRs, the candidate BSR with the higher priority will be elected as the BSR. The range is 0 to 255 and the default priority is 0. **Notes:** When a dynamic RP is used, the candidate BSR must be configured and at least one candidate BSR must be configured in the IPv6 PIM-SM domain.
Static RP	When there's only one Rendezvous Point (RP) in the network, you're suggested to configure a static RP rather than a dynamic RP to save the bandwidth occupied by frequent message exchange between the Candidate RP and the BSR. In the IPv6 PIM-SM domain, the static RP configured on all the devices should be the same. Click **New**. Enter the IPv6 address of the interface where the static RP resides in the **Interface IP** textbox

Option	Description
	and the multicast address in the **Multicast Address** textbox.
RPT to SPT Switchover	Click the switch button to enable RPT to SPT Switchover. Since the RPT (Rendezvous Point Tree) in the IPv6 PIM-SM domain may not be the shortest path, when the multicast data traffic becomes too high, the RP may become the fault point. To solve the problem, by default, the RPT can be switched to the SPT (Shortest Path Tree). After the switchover, the multicast data can be sent directly from the multicast source to the receiver along the SPT. You can switch RPT to SPT as needed.

4. Click **OK**.
5. To delete configured PIMv6, select a virtual router from the **Virtual Router** drop-down list. Click **Delete PIMv6** to delete PIMv6 configuration in this VR.

To configure IPv6 PIM-SM on interfaces, take the following steps:

1. Select **Network** > **Routing** > **PIMv6**.
2. Click **Interface Configuration** in the upper-right corner.

3. Double-click the interface or select the check box before the interface and click **Edit**.



Option	Description
Interface	Displays the name of the interface.
PIM-SM	Turn on the switch button to enable IPv6 PIM-SM.
DR Priority	Specifies the priority of DR. The larger the value is , the higher the priority will be. The default value is 1. The value range is 0 to 4,294,967,294. The priority of the DR (Designated Router) is used to determine which router to use as the designated router (DR). All routers in the IPv6 PIM-SM domain can be specified as DR and the router with higher priority will be selected. If the priority is the same, the one with a larger IP address will be selected.
Hello Interval	With IPv6 PIM-SM enabled, the interface periodically sends Hello packets. You can specify the interval for sending Hello

Option	Description
	packets on the interface as needed. The value range is 1 to 3600 seconds. The default value is 30 seconds.
MLD Query Interval	Specifies the interval for sending MLD general query messages. The range is 1 to 1,800 seconds, and the default value is 125 seconds. The network where the receiver host is located may connect to multiple multicast routers. These multicast routers then elect a router as the querier automatically to maintain MLD group membership of the interface. After the IPv6 PIM-SM function is enabled for the interface, the querier will send MLD host query messages to learn about the entry and exit of multicast group members.
MLD Querier Timeout	Specifies the timeout value for MLD querier. The range is 3 to 3,620 seconds, and the default value is 260 seconds. If the multicast router in the network does not receive MLD query messages within the specified timeout period, multicast routers will elect a querier again.
MLD Query Max Response Time	Specifies the maximum response time for MLD general query. The range is 1 to 32 seconds, and the default value is 10 seconds. You can specify the maximum response time after the receiver host receives the general query message. If no response from the receiver host within the specified maximum response time, the system will delete this receiver in the multicast routing table.

4. Click **OK**.

Viewing PIMv6 Routing Information

To view the multicast routing table, take the following steps:

1. Select **Network** > **Routing** > **PIMv6**.
2. Select a virtual router from the **Virtual Router** drop-down list.
3. Select the **Multicast Routing Table** tab to view the source address, multicast address, ingress interface, and egress interface of the multicast routing.

Chapter 7 Authentication

Authentication is one of the key features for a security product. When a security product enables authentication, the users and hosts can be denied or allowed to access certain networks.

From a user's point of view, authentication is divided into the following categories:

- If you are a user from an internal network who wants to access the Internet, you can use:
  - "Web Authentication" on Page 470
  - "Single Sign-On" on Page 485
  - "802.1x" on Page 536
  - "PKI" on Page 542
- If you are a user from the Internet who wants to visit an internal network (usually with VPN), you can use:
  - "SSL VPN" on Page 605
  - "IPSec VPN" on Page 556 (IPSec VPN (with radius server)+Xauth)
  - "L2TP VPN" on Page 711 (L2TP over IPsec VPN)

Authentication Process

A user uses his/her terminal to connect to the firewall. The firewall calls the user data from the AAA server to check the user's identity.



- User (authentication applicant): The applicant initiates an authentication request, and enters his/her username and password to prove his/her identity.
- Authentication system (i.e. the firewall in this case):The firewall receives the username and password and sends the request to the AAA server. It is an agent between the applicant and the AAA server.
- "AAA Server" on Page 912: This server stores user information like the username and password, etc. When the AAA server receives a legitimate request, it will check if the applicant has the right to the user network services and send back the decision. For more information, refer to "AAA Server" on Page 912. AAA server has the following six types:
  - Local server
  - Radius server
  - LDAP server
  - AD server
  - TACACS+server
  - OAuth2 server

Web Authentication

After the Web authentication (WebAuth) is configured, when you open a browser to access the Internet, the page will redirect to the WebAuth login page. According to different authentication modes, you need to provide corresponded authentication information. With the successful Web authentication, system will allocate the role for IP address according to the policy configuration, which provides a role-based access control method.

Web authentication means you will be prompted to check the identity on the authentication page. It includes the following four modes:

- Password Authentication: Using username and password during the Web authentication.
- SMS Authentication: Using SMS during the Web authentication. In the login page, you need to enter the mobile number and the received SMS verification code. If the SMS verification code is correct, you can pass the authentication.
- NTLM Authentication: System obtains the login user information of the local PC terminal automatically, and then verifies the identity of the user. For more configurations, see NTLM Authentication.
- OAuth2 Authentication: You need to click the OAuth2 authentication icon on the login page of Web authentication to go to the login page of the OAuth2 server. After you enter the user-name and password for the OAuth2 server, you can pass the authentication.



Notes: NTLM authentication mode only supports the Active Directory servers deployed in Windows Server 2008 or older versions.

Enabling the WebAuth

To enable the Web authentication, take the following steps:

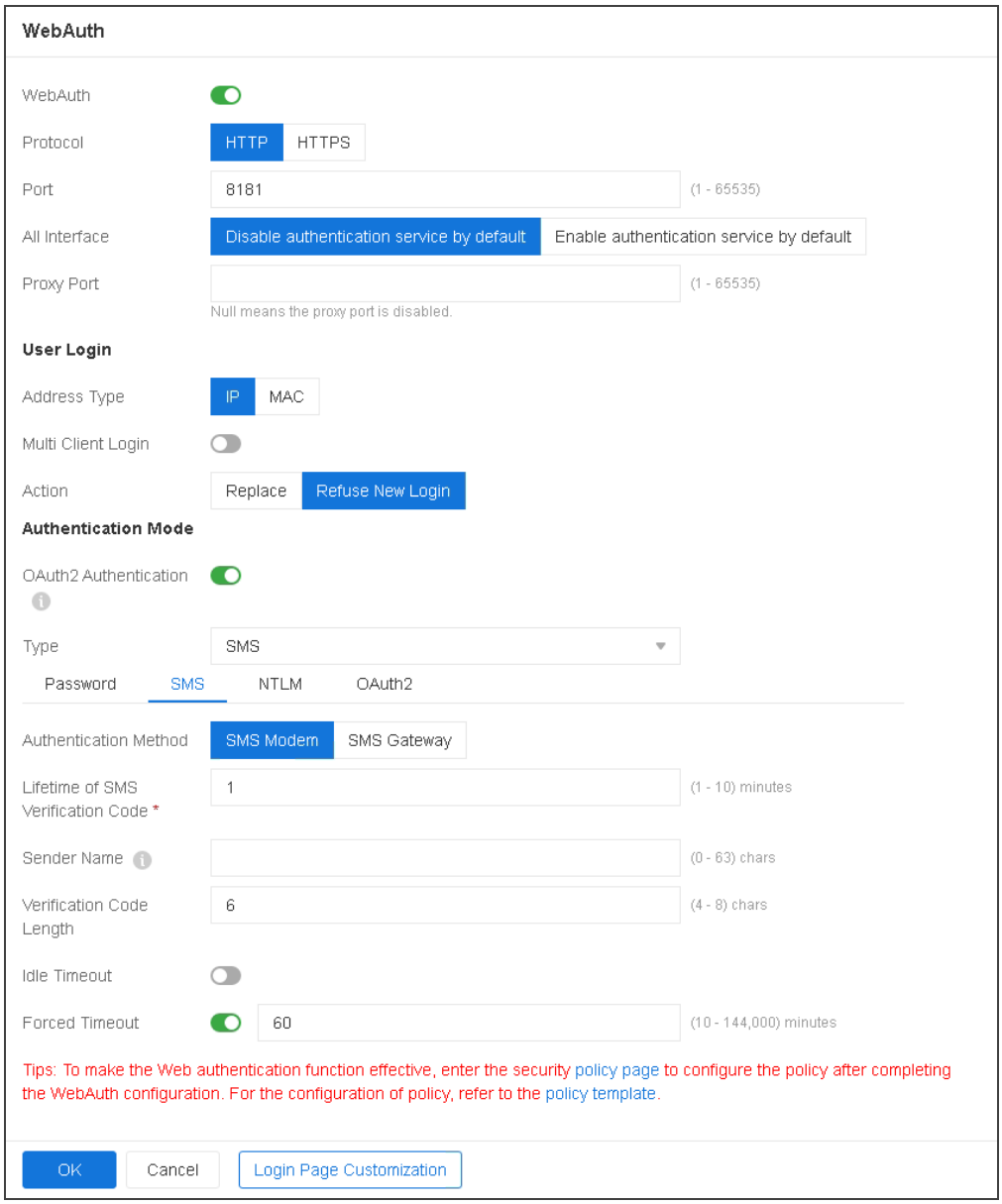
1. Click **Network > WebAuth > WebAuth**.
2. Select the **Enable** check box of **WebAuth** to enable the WebAuth function.

Configuring Basic Parameters for WebAuth

The basic parameters are applicable to all WebAuth polices.

To configure WebAuth basic parameters, take the following steps:

1. Click **Network > WebAuth > WebAuth**,click the **Enable** button.



2. In the Basic Configuration tab, configure the following options

Basic Configuration	
HTTP	Select the HTTP authentication methods. Port: Specifies the HTTP protocol transmission port number of the authentication server. The

Basic Configuration	
	range is 1 to 65535, and the default value is 8181.
HTTPS	Select the HTTPS authentication methods. HTTPS is encrypted, and can avoid information leakage. Port: Specify the HTTPS protocol transmission port number of the authentication server. The range is 1 to 65535, and the default value is 44433. Trust Domain: Specifies the HTTPS trust domain. This domain is previously created in PKI and has imported international CA certified certificate. Certificate Chain: Specifies the name of the HTPPS certificate chain. This certificate chain is already configured in the system. After the certificate chain is configured, when Web authentication is triggered by HTTPS traffic, the firewall will send a digital signature of the certificate from the certificate chain to the client. This certificate, along with the root CA certificate installed on the client, forms a complete certificate trust chain. If all the certificates along the trust chain are valid, the browser on the client considers the certificate of the current user valid and trusted, and no "Your connection is not private" warning message will be displayed. For more information about how to configure a certificate chain, see the **Authentication > PKI > Configuring a Certificate Chain** topic. **Notes:** If an HTTPS certificate chain is specified, take note of the following items: • The levels of the certificate chain constituted by the firewall and the client needs to be con-

Basic Configuration	
	 secutive. For example, for a level-3 certificate chain, if the certificate chains configured on the firewall are level 2 and level 3, the certificate chain installed on the client needs be level 1. • The client needs to be installed with the root CA certificate of the certificate chain. • If you have configured an HTTPS trust domain before configuring an HTTPS certificate chain, you need to cancel the configuration of the trust domain first. • The HTTPS certificate chain has a higher priority than the default trust domain. • The certificate of the certificate chain configured on the firewall needs to contain the item "User Optional Name", which is the IP address or domain name of the interface that has the Web Authentication function enabled.
All Interface	After the WebAuth function is enabled, the WebAuth function of all interfaces is disabled by default. You can specify the Webauth global default configuration of all interfaces, including **Disable authentication service by default** and **Enable authentication service by**

Basic Configuration	
	default. For more information about configuring the WebAuth of interface, see "Configuring an Interface" on Page 158.
Proxy Port	Specifies the port number for HTTPS, HTTPS and SSO proxy server. The port number applies to all. If it changes in any page, the other mode will also use the new port. The range is 1 to 65535.
User Login	
Address Type	Specifies IP address or MAC address as the address type of authentication user. By default, the address type of authentication user is IP address **Note**: When the MAC is specified as the address type of authentication user, the device needs to be deployed in the same Layer 2 network environment with the client. Otherwise, system will fail to get the MAC address of the client or get an incorrect MAC address.
Multiple Login	If you disable the multiple login, one account cannot login if it has already logged in elsewhere. You can click **Replace** to kick out the registered user or you can click **Refuse New Login** to prevent the same user from logging in again. If you enable multiple login, more than one clients can login with the same account. But you can still set up the maximum number of clients using one account.
Authentication Mode	
Password: Specifies the password authentication mode as the authentication mode.	
Idle	If there is no traffic during a specified time period after the suc-

Basic Configuration	
Timeout	cessful authentication, system will disconnect the connection. By default, system will not disconnect the connection if there is no traffic after the successful authentication. Select the **Idle Timeout** check box to enable the idle timeout function, and type the idle timeout value into the text box. Clear the check box to disable the idle timeout function.
Force Timeout	If the forced re-login function is enabled, users must re-login after the configured interval ends. Select the **Force Timeout** check box to enable the forced timeout function, and type the forced timeout value into the text box. Clear the check box to disable the forced timeout function.
Heartbeat Timeout	When authentication is successful, the system will automatically refresh the login page before the configured timeout value ends in order to maintain the login status. If configuring the idle time at the same time, you will log off from the system at the smaller value. Select the **Heartbeat Timeout** check box to enable the heartbeat timeout function, and type the heartbeat timeout value into the text box. Clear the check box to disable the heartbeat timeout function.
Re-Auth Interval	System can re-authenticate a user after a successful authentication. By default, the re-authentication function is inactive. Select the **Re-Auth Interval** check box to enable the re-auth function, and type the re-auth interval into the text box. Clear the check box to disable the re-auth function.
Redirect	The redirect URL function redirects the client to the specified URL

Basic Configuration	
URL	after successful authentication. You need to turn off the pop-up blocker of your web browser to ensure this function can work properly. Notes: • You can specify the username and password in the URL address. When the specified redirect URL is the application system page with the authentication needed in the intranet, you do not need the repeat authentication and can access the application system. The corresponding keywords are $USER, $PWD, or $HASHPWD. Generally, you can select one keyword between $PWD and $HASHPWD. The formart of the URL is "URL" +"username=$USER&password=$PWD". • When entering the redirect URL in CLI, add double quotations to the URL address if the URL address contains question mark. For example, "http://192.10.5.201/oa/-login.-do?username=$USER&password=$HASHPWD"
SMS: Specifies the SMS authentication mode as the authentication mode.	

Basic Configuration	
Authentic-ation Method	Select the method to send authentication SMS, SMS Modem or SMS Gateway.
Lifetime of SMS Veri-fication Code	When using SMS authentication, users need to use the SMS veri-fication code received by the mobile phone, and the verification code will be invalid after the timeout value reaches. After the timeout value reaches, if the verification code is not used, you needs to get the new SMS verification code again. Specifies the verification code interval, the range is 1 to 10 minutes. The default value is 1 minute.
Sender Name	The user can specify a message sender name to display in the mes-sage content. Specifies the sender name. The range is 1 to 63. **Note**: Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information plat-form.
Sign Name	If an ALIYUNSMS service provider name is specified for the "SMS Gateway Name" option, the sign name must be entered in this field and will be displayed in the message content. The range is 1 to 63 characters. This parameter should be the same with the sign name applied in the SMS of Alibaba Cloud.
Veri-fication Code	Specifies the length of the SMS verification code. The range is 4 to 8 characters. The default value is 6.

Basic Configuration	
Length	
Template Code	If the protocol type of the SMS Gateway is ALIYUNSMS, the code of the SMS template must be entered in this field. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the SMS of Alibaba Cloud.
Idle Timeout	If there is no traffic during a specified time period after the successful authentication, system will disconnect the connection. By default, system will not disconnect the connection if there is no traffic after the successful authentication. Select the **Idle Timeout** check box to enable the idle timeout function, and type the idle timeout value into the text box. Clear the check box to disable the idle timeout function.
Force Timeout	If the forced re-login function is enabled, users must re-login after the configured interval ends. Select the **Force Timeout** check box to enable the forced timeout function, and type the forced timeout value into the text box. Clear the check box to disable the forced timeout function.
NTLM: Specifies the NTLM authentication mode as the authentication mode.	
Idle Timeout	If there is no traffic during a specified time period after the successful authentication, the system will disconnect the connection. By default, the system will not disconnect the connection if there is no traffic after the successful authentication. Select the **Idle Timeout** check box to enable the idle timeout function, and type the idle timeout value into the text box. Clear the check box to disable the

Basic Configuration	
	idle timeout function.
Force Timeout	If the forced re-login function is enabled, users must re-login after the configured interval ends. Select the **Force Timeout** check box to enable the forced timeout function, and type the forced timeout value into the text box. Clear the check box to disable the forced timeout function.
When NTLM Fails	It will define the next action when user fails to pass SSO login. Select **Use Password Mode**, and the next step is to use password authentication to continue authentication. Select **No Action**, and the users will fail to login in.
Password/ SMS: Specifies the password authentication or the SMS authentication as the authentication mode.	
Password	Click the **Password** tab, and configure the related parameters for password authentication . For description of options, see "Password" section.
SMS	Click the **SMS** tab, and configure the related parameters for SMS authentication . For description of options, see "SMS" section.
SMS: Specifies the SMS authentication mode.	
SMS	Click the **SMS** tab, and configure the related parameters for SMS authentication . For description of options, see "SMS" section.
OAuth2 Authentication: Click the **Enable** button to enable OAuth2 authentication. By default, this button is disabled. After this function is enabled, click the OAuth2 tab to specify the parameters. The	

Basic Configuration	
OAuth2 authentication can be used together with one of the SMS authentication mode, password authentication mode, and password/SMS authentication mode.	
OAuth2 Server	Specifies the OAuth2 server used for OAuth2 authentication.
Idle Timeout	The maximum time that the Authentication Success page can remain connected in an idle state. Once the idle timeout is exceeded, the connection is closed. To enable this function, turn on the switch next to **Idle Timeout** and enter the idle timeout period. To disable this function, turn off the switch.
Forced Timeout	The system can force users to log on again after a period of time. To enable this function, turn on the switch next to **Forced Timeout** and enter the interval of forcing users to log on again. To disable this function, turn off the switch.
Heartbeat Timeout	After successful authentication, the system will automatically refresh the Authentication Success page before the timeout period expires to confirm the login information. To enable this function, turn on the switch next to **Heartbeat Timeout** and enter the timeout period of the client. To disable this function, turn off the switch.

3. Click **OK**.



Notes:

- If the WebAuth success page is closed, you can log out not only by timeout, but also by visiting the WebAuth status page (displaying online

users, online times and logout button). You can visit it through "http (https):// IP-Address: Port-Number". In the URL, IP-Address refers to the IP address of the WebAuth interface, and Port-Number refers to HTTP/HTTPS port. By default, the HTTP port is 8181, the HTTPS port is 44433. The WebAuth status page will be invalid if there are no online users on the client or the WebAuth is disabled.

- After basic configurations, you should create two policy rules in "Security Policy" on Page 1089 to make WebAuth effective, and then adjust the priority of the two policies to the highest. The WebAuth policies need to be configured according to the following policy template:

Policy Template(Ensure DNS traffic is permitted and enable WebAuth)

Source Z...	Destinatio...	Source A...	Destinati...	User	Service	Action
Any	Any	Any	Any		DNS	Permit
Any	Any	Any	Any	unknown	Any	WebAuth

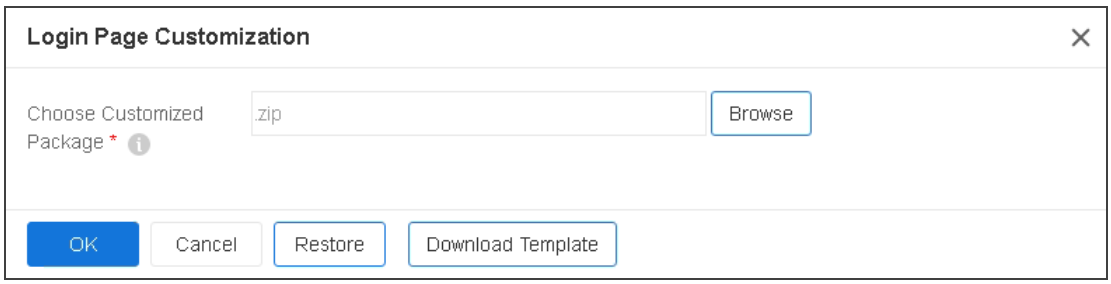
- After WebAuth is configured, the users who matched the WebAuth policy are recommended to input the correct username and password, and then the users can access the network. System takes actions to avoid illegal users from getting usernames and passwords by brute-force. If one fails to log in through the same host three times in two minutes, that host will be blocked for 2 minutes.

Customizing WebAuth Page

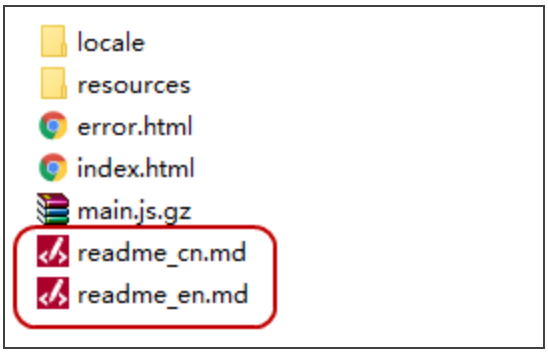
The WebAuth page is the redirected page when an authenticated user opens the browser. By default, you need to enter the username and password in the WebAuth page. You can also select the SMS authentication mode .

1. Click **Network > WebAuth > WebAuth**.

2. Click **Login Page Customization** tab, and click **Download Template** to download the zip file "webauth" of the default WebAuth login page, and then unzip the file.



3. Open the source file and modify the content(including style, picture, etc.)according to the requirements. For more detailed information, see the file of **readme_cn.md** or **readme_en.md**.



4. Compress the modified file and click **Upload** to upload the zip file to system.

Notes:

- After upgrading the previous version to the 5.5R6 version, the WebAuth login page you already specified will be invalid and restored to the default page. You should re-download the template after the version upgrade and customize the login page.

- After upgrading the system version, you should re-download the template, modify the source file, and then upload the custom page compression package. If the uploaded package version is not consistent with the current system version, the function of the custom login page will not be used normally.
- The zip file should comply with the following requirements: the file format should be zip; the maximum number of the file in the zip file is 50; the upper limit of the zip file is 1M; the zip file should contain “index.html”.
- System can only save one file of the default template page and the customized page. When you upload the new customized page file, the old file will be covered. You are suggested to back up the old file.
- If you want trigger WebAuth through HTTPS request, you need import the root certificate (certificate of the device) to the browser firstly. Triggering WebAuth through HTTPS requests depends on the feature of SSL proxy . If the devrice does not support the SSL proxy. Triggering WebAuth through HTTPS requests will not work and you can then trigger WebAuth through HTTP requests.

NTLM Authentication

This method still needs to trigger the browser, and the browser will send user information to the AD server automatically.

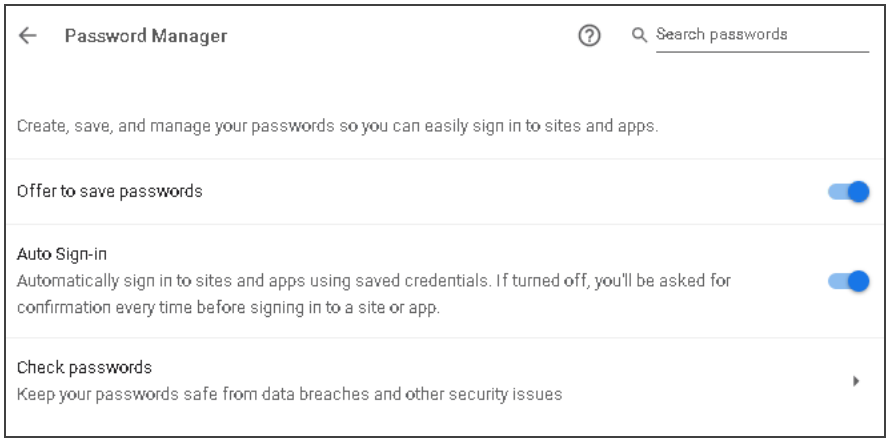
To configure the NTLM authentication, take the following two steps:

Step 1: Configure NTLM for System

1. Click **Network > WebAuth > WebAuth** to enter the WebAuth page.
2. Select **NTLM** from the **Authentication Mode** drop-down list. For the basic configurations, see Configuring Basic Parameters for WebAuth.
3. Click **Apply**.

Step 2: Configure settings for User Browser

1. On the PC terminal of a user, open a browser (take Google Chrome as an example).
2. On the menu bar of Chrome browser, select **Settings** > **Autofill** > **Password Manager**.
3. On the **Password Manager** page, enable **Auto Sign-in**.



4. Log off from the system and logon again, and you can gain access to network resources without WebAuth in Chrome.

Single Sign-On

When the user authenticates successfully for one time, system will obtain the user's authentication information. Then the user can access the Internet without authentication later.

SSO can be realized through three methods, which are independent from each other, and they all can achieve the "no-sign-on"(don't need to enter a user name and password) authentication.

Method	Installing Software or Script	Description
SSO Radius	---	After enabling SSO Radius function, system can receive the accounting packets that based on Radius standard protocol. System will obtain user authentication information, update online user information and manage user's login and logout according to the packets.
SSO Web	---	After you enable SSO Web, the SSO Web client (third-party authentication system) can send user login and logout messages as well as user information update messages to the StoneOS system by using HTTP(S) RESTful API requests. The StoneOS system obtains user authentication information based on the messages to update user information online and manage user login and logout. This enables SSO and policy control based on user groups and roles.
AD Scripting	Logonscript.exe	This method needs to install the script "Logonscript.exe" on the AD server. The triggered script can also send user information to StoneOS. This method is recommended if you have a higher accuracy requirement for statistical monitoring and don't mind to change the AD server.
Radius Snooping	---	The Remote Authentication Dial-In Up Ser-

Method	Installing Software or Script	Description
		vice (RADIUS) is a protocol that is used for the communication between NAS and AAA server. The RADIUS packet monitoring function analyzes the RADIUS packets that are mirrored to the device and the device will automatically obtain the mappings between the usernames of the authenticated users and the IP addresses, which facilitates the logging module for providing the auditing function for the authenticated users.
Agile controller		When Agile Controller is enabled, the system can receive packets sent by the Agile Controller server. The packets are sent when users log in to or log out of the server or when users update their information. The system obtains user authentication information, updates online user information, and manages users' login and logout according to the packets.
AD Polling	---	After enabling the AD Polling function, system will regularly query the AD server to obtain the login user information and probe the terminal PC to verify whether the users are still online, thus getting correct authentication user information to achieve SSO.

Method	Installing Software or Script	Description
		This method is recommended if you don't want to change the AD server.
SSO Monitor	---	After enabling SSO Monitor, StoneOS will build connection with the third-party authentication server through SSO-Monitor protocol, as well as obtain user online status and information of the group that user belongs to. System will also update the mapping information between user name and IP in real time for online user.
TS Agent	Hillstone Terminal Service Agent	This method needs to install and run Hillstone Terminal Service Agent in the Windows server. After the TS Agent is configured, when users log in the Windows server using remote desktop services, the Hillstone Terminal Service Agent will allocate port ranges to users and send the port ranges and users information to the system. At the same time, the system will create the mappings of traffic IPs, port ranges and users, and achieve the "no-sign-on" authentication.

Enabling SSO Radius for SSO

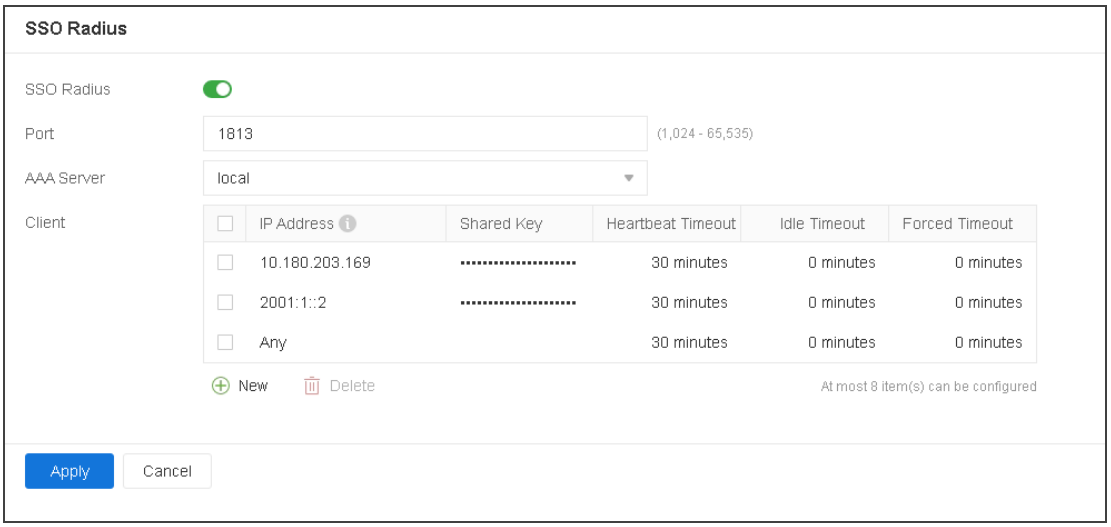
After enabling SSO Radius function, system can receive the accounting packets that based on Radius standard protocol. System will obtain user authentication information, update online user

information and manage user's login and logout according to the packets.

To configure the SSO Radius function, take the following steps:

1. Click **Object >SSO Server >SSO Radius** and enter **SSO Radius** page. By default, SSO Radius is disabled. After enabling SSO Radius, you should wait at least 5 seconds before disabling it, and vice versa. During workload peaks, the waiting time may be extended.

2. Click the **Enable** button to enable the SSO Radius function.



3. Specify the Port to receive Radius packets for StoneOS (Don’t configure port in non-root VSYS). The range is 1024 to 65535. The default port number is 1813.

4. Specify the AAA Server that user belongs to. You can select the configured Local, AD or LDAP server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.

5. Specify the IP Address, Shared Secret and Idle Interval of SSO Radius client which is allowed to access system. You can configure up to 8 clients.

    - IP Address: Specify the IPv4 address or the IPv6 address (the IPv6 address is valid only when the system version is the IPv6 version) of SSO Radius client. If the

address is specified as "any", it means that system receives the packets sent from any Radius client.

- Shared Key: Specify the shared secret key of SSO Radius client. The range is 1 to 31 characters. System will verify the packet by the shared secret key, and parse the packet after verifying successfully. If system fails to verify the packet, the packet will be dropped. The packet can be verified successfully only when SSO Radius client is configured the same shared secret key with system or both of them aren't configured a shared secret key.
- Heartbeat Timeout(minute): Configure the idle interval for the authentication information of Radius packet in the device. If there’s no update or delete packet of the user during the idle interval, the device will delete the user authentication information. The default value is 30. 0 means the user authentication information will never timeout. If heartbeat timeout and idle timeout is configured at the same time, the user will logout at the minimum time point between the heartbeat timeout and the idle timeout.
- Idle Timeout: Idle timeout refers to the longest time during which the authenticated user keeps his/her authenticated state in non-traffic state. When the configured idle timeout is exceeded, system will delete the authentication information of the user. The unit is minute. The range is from 0-1440. The default value is 0. If it is specified as 0, this function will be disabled, which means the authenticated user will not be kicked out in non-traffic state.
- Forced Timeout: When the online time of a user exceeds the configured force timeout time, system will kick out the user and force the user to log out. The range is 0 to 144000 minutes, and the default value is 600 minutes. If it is specified as 0, this function will be disabled.

6. Click **Apply** button to save all the configurations.

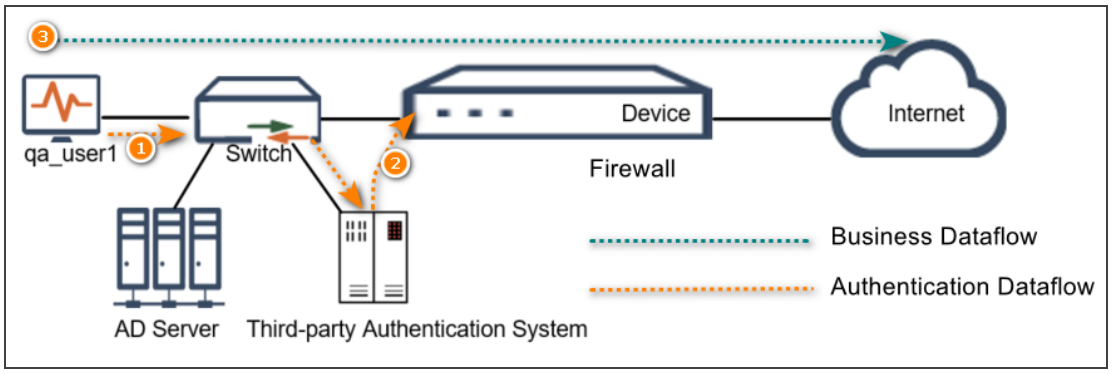
SSO Web for SSO

The firewall supports integration with a third-party authentication system by using the SSO Web function to achieve SSO and policy control based on user groups and roles. This includes:

- The firewall is integrated with a third-party authentication system, which sends user login/-logout messages and user information update messages to the firewall via HTTP(S) RESTful API requests. The firewall retrieves user authentication information based on these messages.
- When an authenticated user accesses the firewall, the firewall uses the synchronized authentication information to update online user information and manage user login/logout operations, thereby achieving SSO and policy control based on user groups and roles.

Typical Scenarios of SSO Web for SSO

The typical scenario of SSO Web for SSO is as follows:



1. Users use a third-party authentication system for authentication.
2. The third-party authentication system sends user authentication information to the firewall via HTTP(S) RESTful API requests.

   The method by which the firewall obtains the user group or role information depends on the sent user authentication messages and the configuration of the AD server on the firewall.

There are four possible scenarios:

- If the user authentication information sent to the firewall **includes user group or role information**, the firewall directly retrieves the user group or role information;
- If the user authentication information sent to the firewall **does not include user group information**, and the AD server on the firewall is configured to synchronize both users and user groups, the firewall can query the user group to which the user belongs from the synchronized data in the AD server;
- If the user authentication information sent to the firewall **does not include user group information**, and the AD server on the firewall is configured to synchronize only users, only user groups, or neither users nor user groups, the firewall can query the user group to which the user belongs by using the AD server;
- If the user authentication information sent to the firewall **does not include role information**, but the firewall has a role mapping rule configured for the AD server, the firewall can assign a role to the user based on the mapping rules.

3. The firewall provides network access control for users based on user groups or roles, and users do not need to be authenticated again for network access.

Configuring SSO Web for SSO

To configure SSO Web for SSO, follow this procedure:

1. Configure the AAA server referenced by SSO Web: Local, Active-Directory, or LDAP servers.
2. Configure SSO Web in the Firewall.
3. Constructing an HTTP(S) RESTful API Request in the Third-Party Authentication System.

Configuring SSO Web for SSO

To configure SSO Web for SSO, take the following steps:

1. Select **Object** > **SSO Server** > **SSO Web**. By default, SSO Web is disabled.
2. Click the **Enable** button to enable SSO Web.



3. Specify the AAA server where the user belongs. After you select an AAA server, the system can query the user group and role information corresponding to the username of online user on the referenced AAA server. This implements user group and role-based policy control. From the drop-down list, you can search for and select the existing Local, AD, or LDAP server. To create a server, click ⊕. For more information about how to configure the server, see "AAA Server" on Page 912. By default, the Local server is selected.
4. Specify the forced timeout. If the system does not receive the user information update request within the enforced timeout after the user logs in, the user will be forcefully logged out and disconnected. The range is 0 to 1440 minutes, and the default value is 0 minute. If it is set to 0, this function will be disabled.
5. Specify the IP range of the trusted client. Only SSO Web clients within the specified IP range can send user login/logout and user information update messages to the StoneOS system via HTTP(S) RESTful API. From the drop-down list, you can search for and select an

existing IPv4 or IPv6 address book entry in the system. To create an address book entry, click ⊕. For more information about how to configure the entry, see "Address" on Page 814. The default value is "Any", which indicates that any SSO Web client of IPv4 address can send user login/logout and user information update messages to the StoneOS system via HTTP(S) RESTful API.

6. Click **OK**.

Constructing an HTTP(S) RESTful API Request in the Third-Party Authentication System



Notes:

- The firewall interface communicating with a third-party authentication system needs to have HTTP or HTTPS services enabled.
- The IP address of the third-party authentication system need to fall within the trusted host range of the firewall.

The O&M personnel of the third-party authentication system use development tools to construct HTTP(S) RESTful API requests within the code. Upon successful user authentication, the third-party authentication system synchronizes the user authentication information with the firewall.

The formats of RESTful API requests are as follows:

- User login request: http(s)://*firewall's IP*/rest/api/sso-web-user?**opr=login&info=***USERINFO*
- User logout request: http(s)://*firewall's IP*/rest/api/sso-web-user?**opr=logout&info=***USERINFO*

Parameter description:

- *firewall's IP*: The IP address of the firewall receiving user authentication information.
- **opr**: Supports only two message types —**login** and **logout**
- **info**=*USERINFO*: The user information for login or logout. *USERINFO* is a base64-encoded string containing the authenticated user's UserIP, UserName, Group, and Role details, which needs to be generated in the third-party authentication system's code based on the required format. UserIP and UserName are required, while Group and Role are optional. It supports multiple Group but only one Role. The format of USERINFO before encoding is as follows:

Authenticated User Information	USERINFO Format before Encoding
Contains only user IP and username	UserIP/UserName//
Contains user IP, username, and Group	UserIP/UserName//Group
Contains user IP, username, and Role	UserIP/UserName////role=Role
Contains user IP, username, Group, Role	UserIP/UserName//Group//role=Role
Contains user IP, username, multiple Group and Role	UserIP/UserName//Group1//Group2//role=Role

Example: UserIP=120.1.1.163, UserName=qa_user1, Group=QA_Group, Role=RnD-Group. The IP address of the firewall is 10.182.12.34, so USERINFO is "120.1.1.163/qa_user1//QA_Group//role=RnD-Group". After performing base64 encoding in the third-party system, the result is: MTIwLjEuMS4xNjMvcWFfdXNlcjEvL1FBX0dyb3VwLy9yb2xlPVJuRC1Hcm91cA==

Therefore, the login/logout requests from the third-party system are as follows:

- Login request: http(s)://10.182.12.34/rest/api/sso-web-user-

?opr-

=login&i-

nfo-

o=MTIwLjEuMS4xNjMvcWFfdXNlcjEvL1FBX0dyb3VwLy9yb2xlPVJuRC1Hcm91cA==

- Logout request: http(s)://10.182.12.34/rest/api/sso-web-user-

  ?opr-

  =logout&i-

  nfo-

  o=MTIwLjEuMS4xNjMvcWFfdXNlcjEvL1FBX0dyb3VwLy9yb2xlPVJuRC1Hcm91cA==

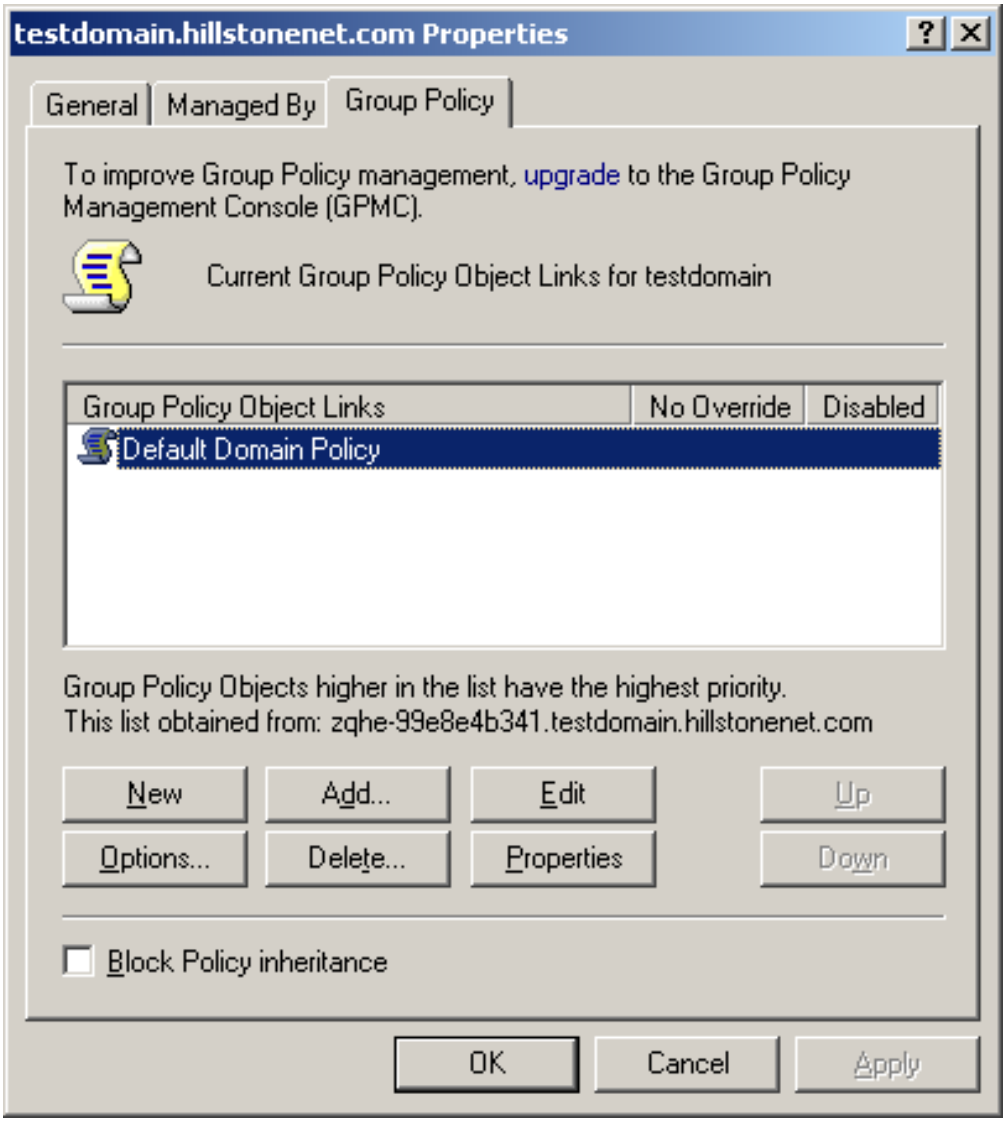
Using AD Scripting for SSO

Before using a script for SSO, make sure you have established your Active Directory server first. To use a script for SSO, take the following steps:

Step 1: Configuring the Script for AD Server

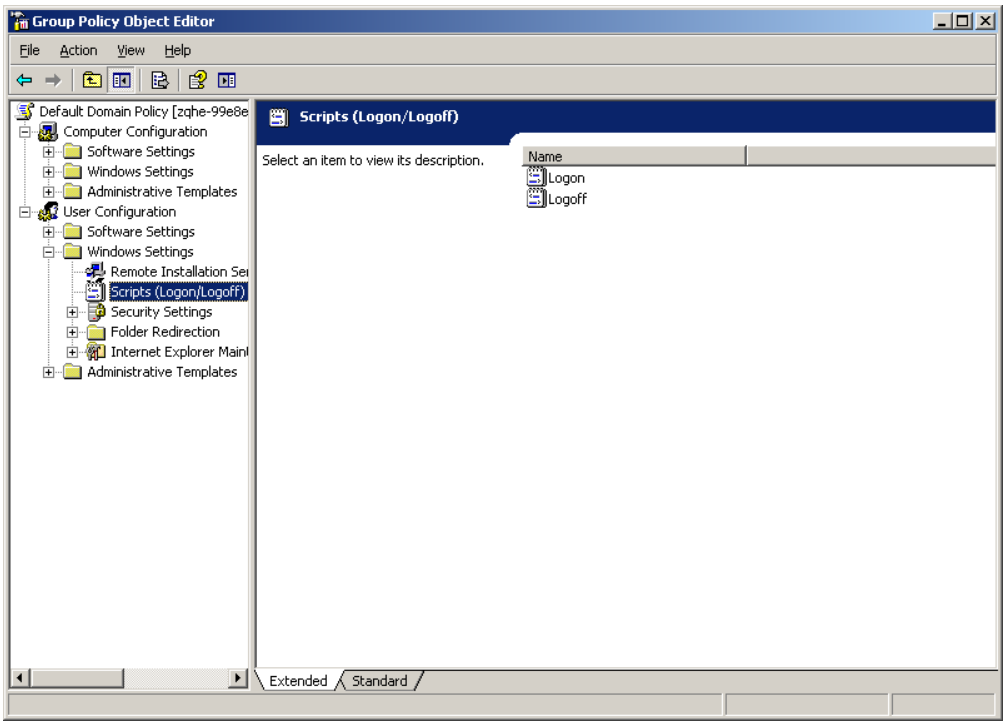
1. Open the AD Security Agent software(for detailed information of the software, see Using AD Agent Software for SSO). On the <AD Scripting> tab, click **Get AD Scripting** to get the script "Logonscript.exe" , and save it in a directory where all domain users can access.
2. In the AD server, enter **Start** menu, and select **Mangement Tools > Active Directory User and Computer**.

3. In the pop-up <Active Directory User and Computer> dialog box, right-click the domain which will apply SSO to select **Properties**, and then click <Group Policy> tab.

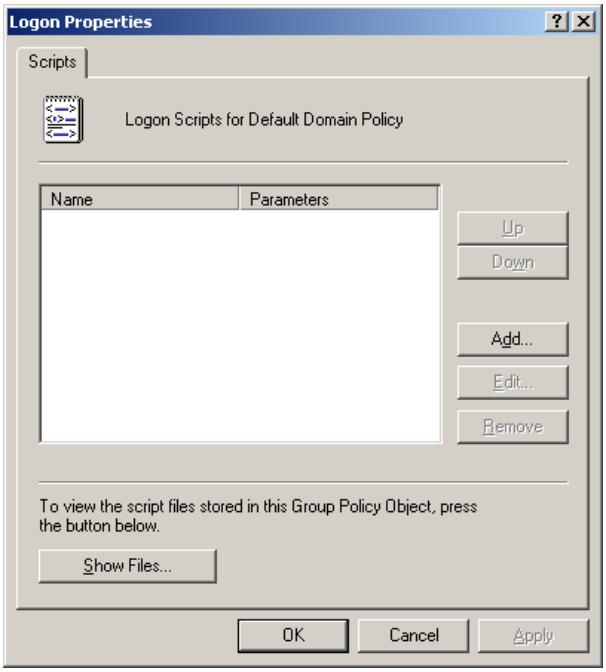


4. In the Group Policy list, double-click the group policy which will apply SSO. In the pop-up <Group Policy Object Editor>dialog box, select **User Configuration > Windows Settings>**

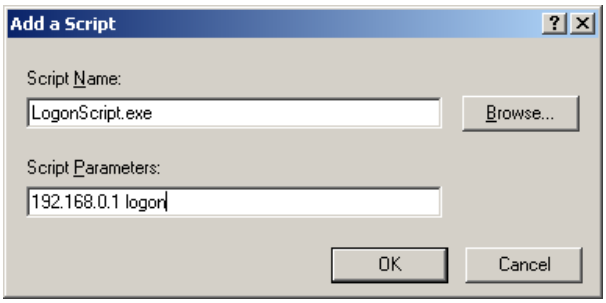
Script (Logon/Logout).



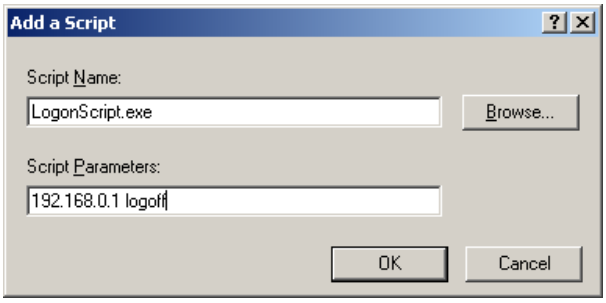
5. Double-click **Logon** on the right window, and click **Add** in the pop-up <logon properties> dialog box.



6. In the <Add a Script> dialog box, click **Browse** to select the logon script (logonscript.exe) for the Script Name; enter the authentication IP address of StoneOS and the text "logon" for the Script Parameters(the two parameters are separated by space). Then, click **OK**.



7. Take the steps of 5-6 to configure the script for logging out, and enter the text "logoff" in the step 6.



Notes: The directory of saving the script should be accessible to all domain users, otherwise, when a user who does not have privilege will not trigger the script when logs in or out.

Step 2: Configuring AD Scripting for StoneOS

After the AD Scripting is enabled, the user can log in Hillstone device simultaneously when logging in the AD server successfully. System only supports AD Scripting of Active Directory server.

To configure the AD Scripting function, take the following steps:

1. Click **Object> SSO Server > AD Scripting** to enter the AD Scripting page. The AD Scripting function is disabled by default.



2. Select the **Enable** button of AD Scripting to enable the function.

3. Specify the AAA Server that user belongs to. You can select the configured Local, AD or LDAP server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.

4. Specify the Idle Interval, which specifies the longest time that the authentication user can keep online without any traffic. After the interval timeout, StoneOS will delete the user authentication information. The value range is 0 to 1440 minutes. 0 means always online.

5. Allow or disable users with the same name to log in depends on needs.

   - **Enable** : Click to permit the user with the same name to log in from multiple terminals simultaneously.
   - **Disable**: Click to permit only one user with the same name to log in, and the user logged in will be kicked out by the user logging in.

6. Click **Apply** to save the changes.

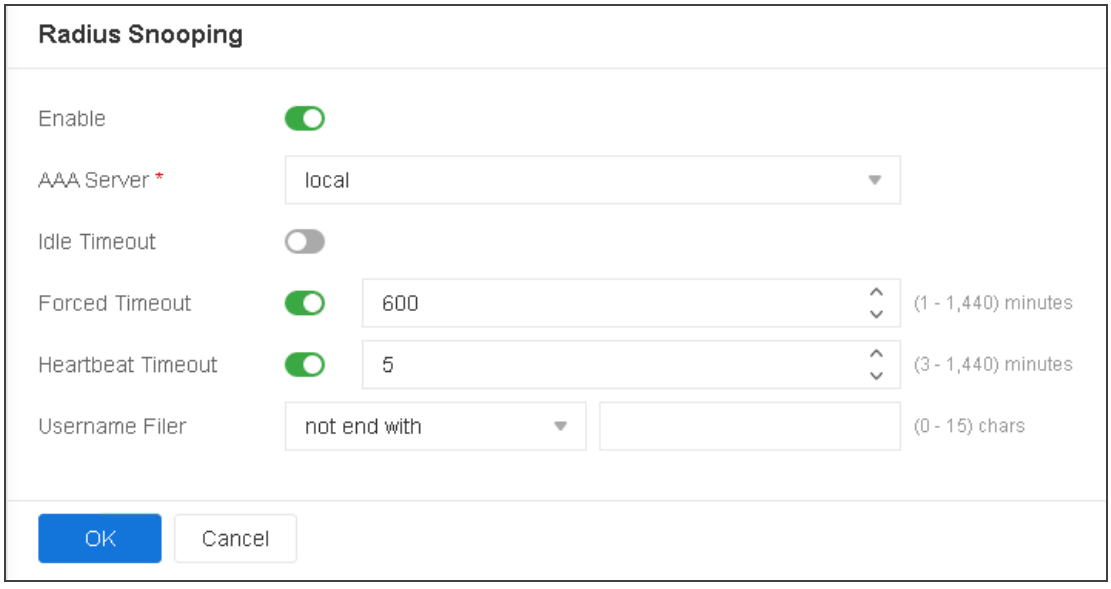
After completing the above two steps, the script can send the user information to StoneOS in real time. When users log in or out, the script will be triggered and send the user behavior to StoneOS.

Radius Snooping

The Remote Authentication Dial-In Up Service (RADIUS) is a protocol that is used for the communication between NAS and AAA server. The RADIUS packet monitoring function analyzes the RADIUS packets that are mirrored to the device and the device will automatically obtain the mappings between the usernames of the authenticated users and the IP addresses. Then the system generates user authentication information and adds it to the authenticated user list to control and audit user traffic.

To configure Radius Snooping, take the following steps:

1. Click **Object> SSO Server > Radius Snooping** to enter the Radius Snooping page. The Radius Snooping function is disabled by default.



2. Select the **Enable** button of Radius Snooping to enable the function.

3. Specify the AAA Server that user belongs to. You can select the configured Local, AD or LDAP server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.

4. Specify the idle time. If the device does not receive the mirrored RADIUS packets within the specified time period, it will delete the mappings between the usernames and the IP addresses. The value ranges from 1 to 1440. By default, system will not delete the user authentication information if there is no traffic.

5. Specify the forced logout time. When the online time of a user exceeds the configured force timeout time, system will kick out the user and force the user to log out. The range is 0 (the function is disabled) to 1440 minutes, and the default value is 600 minutes.

6. Specify the heartbeat timeout value. When authentication is successful, the system will automatically reconfirm login information before the configured timeout value ends in order to maintain the login status. If configuring the idle time at the same time, you will log off from the system at the smaller value. The value range is 3 to 1440 minutes. The default value is 5 minutes.

7. Username Filter: The "not end with" filter condition indicates that usernames ended with a specific string are excluded. The system generates user authentication information only for usernames not excluded by the "not end with" filter condition. The value range of the string is from 1 to 15 characters.

8. Click **Apply** to save the changes.

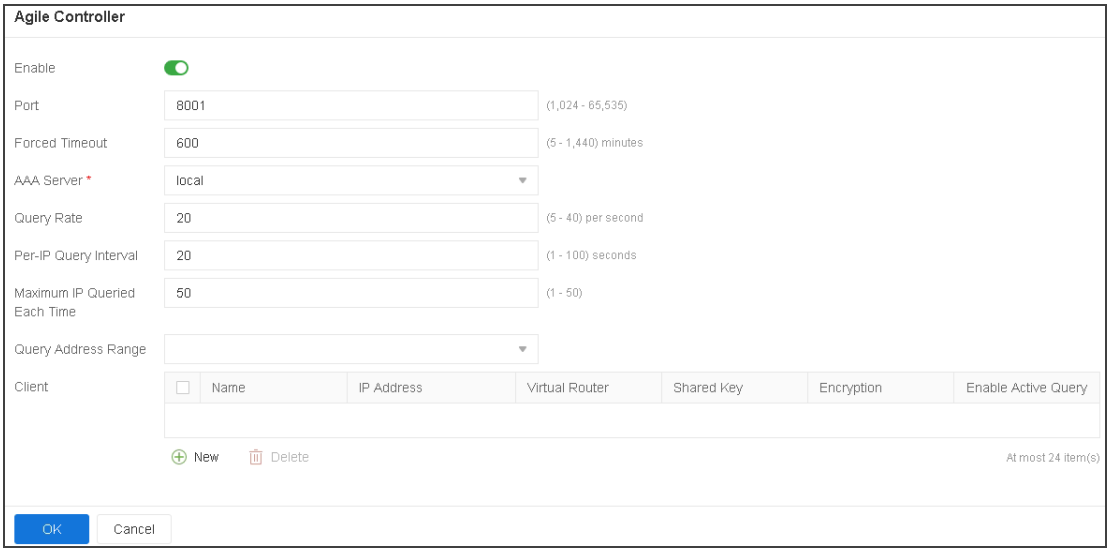
Realizing SSO via Agile Controller

When Agile Controller is enabled, the system can receive packets sent by the Agile Controller server. The packets are sent when users log in to or log out of the server or when users update their information. To realize SSO, the system obtains user authentication information, updates online user information, and manages the user's login and logout according to the packets.

To configure Agile Controller, take the following steps:

1. Click **Object > SSO Server > Agile Controller** to enter the Agile Controller page. By default, Agile Controller is disabled.

2. Click the **Enable** button to enable the Agile Controller function.



Configure the following options:

Option	Description
Port	Specifies the port for StoneOS to receive packets from the Agile Controller server (Port cannot be configured in non-root VSYS). The range is from 1024 to 65535. The default port number is 8001.
Forced Timeout	Specifies the timeout after which access for the authenticated user is forcibly terminated. The range is 5 to1440 minutes. The default timeout is 600 minutes.
AAA Server	Select the AAA Server that the user belongs to. You can select the configured Local, AD, or LDAP server. For more inform-

Option	Description
	ation, see AAA Server. After selecting the AAA server, the system can query the user group and role information associated with the username of the online user on the referenced AAA server, to realize the policy control based on the user group and role.
Query Rate	Specifies the query rate when the system actively sends query packets to the Agile Controller server to acquire the information of the online user associated with the source IP. The range is 5-40 times/second. The default value is 20 times/second.
Per-IP Query Interval	Specifies the query interval between each source IP when the system actively sends query packets to the Agile Controller server to acquire the information of the online user associated with the source IP. The range is 1-100 seconds. The default value is 20 seconds.
Maximum IP Queried Each Time	Specifies the maximum source IPs contained in a query packet when the system actively sends query packets to the Agile Controller server to acquire the information of the online user associated with the source IP. The range is 1-50. The default value is 50.
Query Address Range	Specifies the address range of the source IP to be queried when the system actively sends query packets to the Agile Controller server to acquire the information of the online user associated with the source IP. You can search and select the specified IP from the drop-down list. Click ⊕ to create a new IP.

Option	Description
Client	Click **New** to allow a new Agile Controller client. You can configure at most 24 clients. • Name: Specifies the name of the Agile Controller server. • IP Address: Specifies the IP address of the Agile Controller server. • Virtual Router: Specifies the virtual router that the Agile Controller server belongs to. • Shared Key: The system verifies the encrypted communication packets sent by the Agile Controller server by using the shared key. The system parses the packets only when the verification is successful. Otherwise, the system drops the packets. The Agile Controller client should be configured with the same shared key as the Agile Controller server. Otherwise, the packets cannot be successfully verified. The range is 1-31 characters. • Encryption: Specifies the encryption algorithm applied in the communication between the system and the Agile Controller server. The encryption algorithm can be 3DES or AES128. If this option is not specified, the system uses the AES128 algorithm by default. • Enable Active Query: With this checkbox selected, the system will actively query the information of the online

Option	Description
	users from the Agile Controller server.

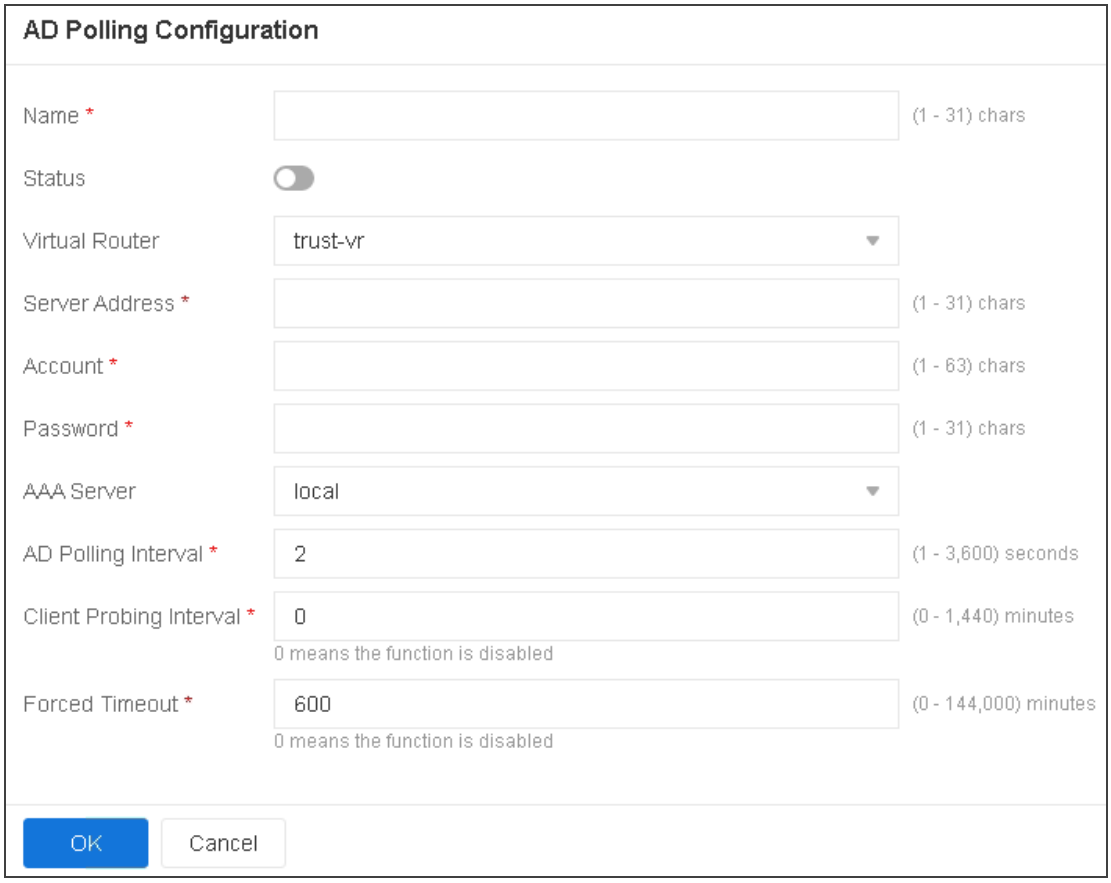
3. Click **OK** to complete the configuration.

Using AD Polling for SSO

When the domain user logs in the AD server, the AD server will generate login logs. After enabling the AD Polling function, system will regularly query the AD server to obtain the user login information and probe the terminal PCs to verify whether the users are still online, thus getting correct authentication user information to achieve SSO.

Before using AD Polling for SSO, you should make sure that the Active Directory server is set up first. To use AD Polling for SSO, take the following steps:

1. Click **Object >SSO Client >AD Polling** to enter the AD Polling page.
2. Click the ⊕ New button on the upper left corner of the page, and the **AD Polling Configuration** dialog box pops up.



Configure the following options:

Option	Description
Name	Specifies the name of the new AD Polling profile. The range is 1 to 31 characters
Status	Click **Enable** button to enable the AD Polling function. After enabling, system will query the AD server to obtain the user information and probe the terminal PC to verify whether the online users are online regularly. When queries for the first time, system will obtain the online user information on the AD server in the previous 8 hours . If fails to obtain the previous inform-

Option	Description
	ation, system will obtain the following online user information directly.
Server Address	Enter the IP address of authentication AD server in the domain. You can only select AD server. After specifying the authentication AD server, when the domain users log in the AD server, the AD server will generate the login logs. The range is 1 to 31 characters.
Virtual Router	Select the virtual router that the AD server belongs to in the drop-down list.
Account	Enter a domain user name to log in the AD server. The format is domain\username, and the range is 1 to 63 characters. The user is required to have permission to query security logs on the AD server, such as the user of Administrator whose privilege is Domain Admins on the AD server.
Password	Enter a password corresponding to the domain user name. The range is 1 to 31 characters.
AAA Server	Select the referenced AAA server in the drop-down list. You can select the configured Local, AD or LDAP server, see "AAA Server" on Page 912. You are suggested to select the configured authentication AD server. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role,.
AD Polling	Configure the interval for regular AD Polling probing. System

Option	Description
Interval	will query the AD server to obtain the online user information at interval. The range is 1 to 3600 seconds, and the default value is 2 seconds. You are suggested to configure 2 to 5 seconds to ensure to obtain online user information in real time.
Client Probing Interval	Configure the interval for regular client probing. System will probe whether the user is still online through WMI at interval, and kick out the user if cannot be probed. The range is 0 to 1440 minutes, and the default value is 0 minute(the function is disabled). You are suggested to configure a larger probing interval to save the system performance, if you have low requirements for the offline users.
Force Timeout	Configure the forced logout time. When the user's online time exceeds the configured timeout time, system will kick out the user and force the user to log out. The range is 0 （the function is disabled） to 144000 minutes, and the default value is 600 minutes.

3. Click **OK** button to finish the configuration of AD Polling.



Notes:

- When system is restarted or the configuration of AD Polling (except the account, password and force timeout) is modified, system will clear the existed user information and obtain the user information according to the new configuration.



- To realize the AD Polling function, you need to enable the WMI of the PC where the AD server is located and the terminal PC. By default, the WMI is enabled. To enable WMI, you need to enter the **Control Panel >Administrative Tools> Services** and enable the WMI performance adapter.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the RPC service and remote management should be enabled. By default, the RPC service and remote management is enabled. To enable the RPC service, you need to enter the **Control Panel >Administrative Tools> Services** and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command **netsh firewall set service RemoteAdmin**.
- To enable WMI to probe the PC where the AD server is located and the terminal PCs, the PC should permit WMI function to pass through Windows firewall. Select **Control Panel >System and Security> Windows Firewall >Allow an APP through Windows Firewall**, in the **Allowed apps and features** list, click the corresponding check box of Domain for Windows Management Instrumentation (WMI) function.
- To use the offline function, you should make sure that the time of the PC where the AD server is located and the terminal PCs is the same. To enable the function of Synchronize with an Internet time server, select **Control Panel > Clock, Language, and Region > Date and Time**, and the Date and Time dialog box pops up. Then, click **Internet Time** tab, and check **Synchronize with an Internet time server**.

Using SSO Monitor for SSO

SSO Monitor can synchronize the online status of users stored on external servers to the firewall based on specified protocol packets, generate authenticated users on the firewall, and update the username-IP (IPv4 or IPv6 address) binding relationship of online users in real time. In addition, SSO Monitor can extract the user group of users from packets so that the users can avoid repetitive login process.

StoneOS does not restrict the form and type of external servers. A server of TCP connection that can synchronize user information to the firewall over the SSO Monitor protocol can be used as an external server, such as AD Agent software.

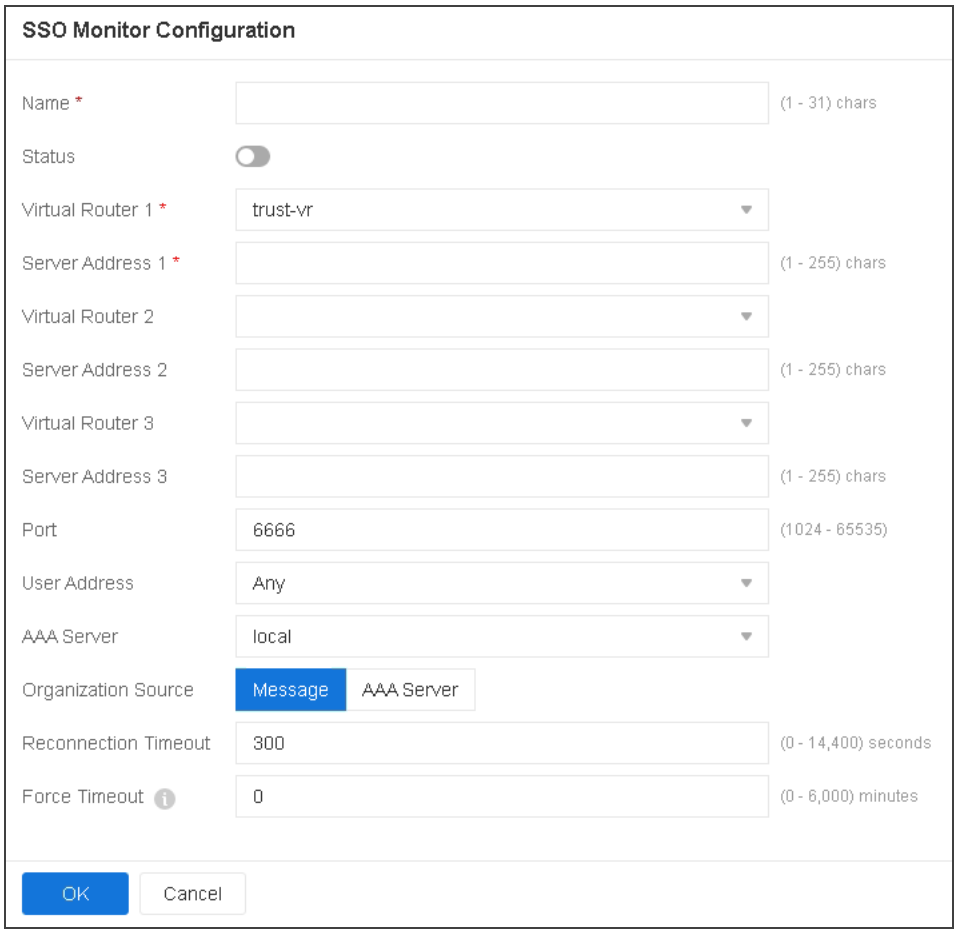


Notes: To use AD Agent software to obtain user information in version earlier than StoneOS 5.5R10, you can connect the AD agent by using SSO Monitor or configure the security agent in Active-Directory server configuration mode. In StoneOS 5.5R10 and later, the system no longer supports the security agent function. When the version is upgraded to StoneOS 5.5R10 or later, the configured security agent function is automatically converted to the SSO Monitor function to connect to the AD Agent software configuration. You can view the configuration on Object > SSO Client > SSO Monitor. The converted name of SSO Monitor is the same as that of the AD server.

To use SSO Monitor for SSO, take the following steps:

1. Click **Object >SSO Client > SSO Monitor** to enter **SSO Monitor** page.

2. Click the ⊕ New button and the **SSO Monitor Configuration** dialog box pops up.



Configure the following options:

Option	Description
Name	Specify the name of the new SSO Monitor. The range is 1 to 31 characters.
Status	Click **Enable** button to enable the SSO Monitor function. After enabling the function, system will build connection with the third-party authentication server through SSO-Monitor pro-

Option	Description
	tocol, as well as obtain user online status and information of group that user belongs to. The machine will generate authentication user according to the authentication information.
Server Address 1	Enter the domain name, IPv4 address, or IPv6 address of the external server. The range is 1 to 255 characters. The external server needs to support sending user online status to the firewall by using the SSO-Monitor protocol. You need to configure at least one external server address 1, 2, or 3. If more than one address is configured, other addresses are used for redundant backup. If an address fails to be connected, the system connects to the next address. We recommend that you configure the addresses in the order of 1, 2, and 3.
Virtual Router 1	Select the virtual router to which the interface of the firewall used to communicate with the backed up external server address 1 belongs.
Virtual Router 2	Select the virtual router to which the interface of the firewall used to communicate with the backed up external server address 2 belongs.
Server Address 2	Enter the domain name, IPv4 address, or IPv6 address of the backed up external server.
Virtual Router 3	Select the virtual router to which the interface of the firewall used to communicate with the backed up external server address 3 belongs.

Option	Description
Server Address 3	Enter the domain name, IPv4 address, or IPv6 address of the backed up external server.
Port	Specifies the port number of the third-party authentication server. System will obtain user information through the port number. The default number is 6666. The range is 1024 to 65535.
User Address	Select the configured address book from the drop-down list. When generating authentication users, the system only generate users within the specified IP range. Click ⊕ to create a new address book.
AAA Server	Select the referenced AAA server in the drop-down list. You can select the configured Local, AD or LDAP server, see "AAA Server" on Page 912 for configuration method. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.
Organization Source	Select the method to synchronize user organization structure with system, including Message and AAA Server. When Message is selected, StoneOS will use the user group of authentication information as the group that user belongs to. It's usually used in the scenario of the third-party authentication server saving user group. When AAA Server is selected, StoneOS will use the user organization structure of AAA server

Option	Description
	as the group that user belongs to. It's usually used in the scenario of the third-party authentication server being authenticated by AAA server and the user organization structure being saved in the AAA server.
Reconnection Timeout	Configure the reconnection timeout. When StoneOS disconnects with the third-party authentication server due to timeout, system will wait during the disconnection timeout. If system still fails to connect within the configured time, it will delete online users. The range is 0 to 1800 seconds. The default value is 300. 0 means the user authentication information will never timeout.
Force Timeout	Specifies the force timeout of SSO Monitor, which is used to control the online duration of authenticated users. Note: If the external server connected to SSO Monitor is an AD Agent software, we do not recommend that you configure this parameter and the user online duration parameter on AD Agent at the same time.

3. Click **OK** button to finish SSO Monitor configuration.



Notes: You can configure different numbers of SSO Monitor on different servers. When the configured number exceeds the limit, system will pops up the alarm information.

Configuration Examples of Using SSO Monitor for SSO

AD Agent software can send user online status within the AD domain to the firewall by using packets of SSO-Monitor protocol. Therefore, AD Agent software can be used as an external

server that connects SSO Monitor for SSO. In this example, AD Agent software is used to show you how to implement SSO by connecting SSO Monitor with AD Agent.

Install AD Agent software on a PC within the AD server or domain. When a user in the domain logs in to the Active-Directory server, AD Agent records the username, IP address, and time when the user was most recently online, and sends the mapping relationships between usernames and IP addresses to StoneOS. This avoids users from repeated logins and generates authenticated users on the firewall. The system can also implements user-based security statistics, log records, and online behavior auditing by using the obtained mapping relationships between usernames and IP addresses.

To use SSO Monitor for SSO, take the following steps:

Step 1: Installing and Running AD Security Agent on a PC or Server

AD Security Agent can be installed on an AD server or a PC in the domain. If you install the software on an AD server, the communication only includes "AD Security Agent →StoneOS"; If you install the software on a PC in the domain, the communication includes both process in the following table. The default protocol and port used in the communication are described as follows:

Communication direction		AD Security Agent→AD Server	AD Security Agent→StoneOS
Protocol		TCP	TCP
Port	StoneOS	---	6666
	AD Security Agent	1935、1984	6666
	AD Server	445	---

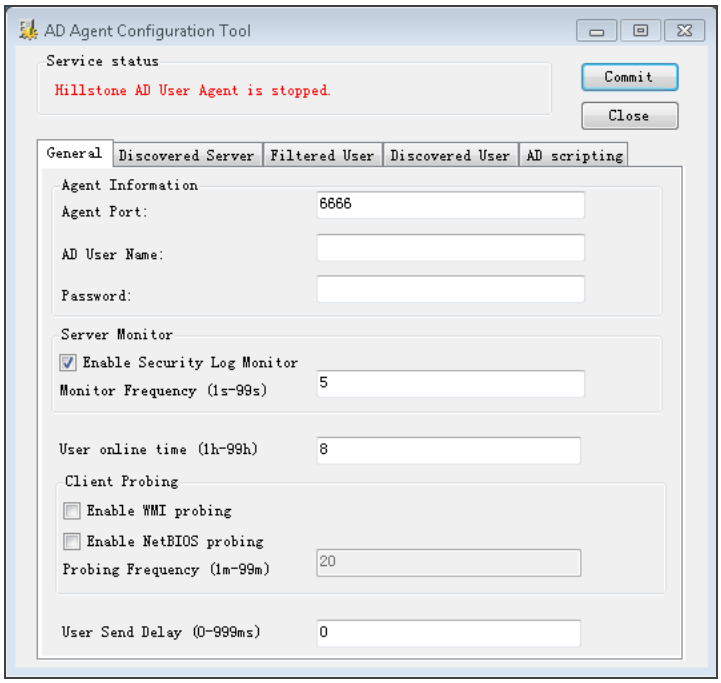
To install the AD Security Agent to an AD server or a PC in the domain, take the following steps:

1. Click http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-adagent to download an AD Security Agent software, and copy it to a PC or a server in the domain.
2. Double-click ADAgentSetup.exeto open it and follow the installation wizard to install it.

3. Start AD Security Agent through one of the two following methods:

   - Double-click the AD Agent Configuration Tool shortcut on the desktop.
   - Click **Start** menu, and select **All app > Hillstone AD Agent >AD Agent Configuration Tool**.

4. Click the <General> tab.



On the <General> tab, configure these basic options.

Option	Description
Agent Port	Enter agent port number. AD Security Agent uses this port to communicate with StoneOS. The range is 1025 to 65535. The default value is 6666. This port must be the same with the configured monitoring port in StoneOS, otherwise, the AD Security Agent and StoneOS cannot communicate with each other.
AD User	Enter user name to log in the AD server. If AD Security Agent

Option	Description
Name	is running on the other PCs of the domain, this user should have high privilege to query event logs in AD server, such as the user of Administrator whose privilege is Domain Admins on AD server.
Password	Enter the password that matched with the user name. If the AD Security Agent is running on the device where the AD server is located, the user name and password can be empty.
Server Monitor	
Enable Security Log Monitor	Select to enable the function of monitoring event logs on AD Security Agent. The default query interval is 5 seconds. The function must be enabled if the AD Security Agent is required to query user information.
Monitor Frequency	Specifies the polling interval for querying the event logs on different AD servers. The default value is 5 seconds. When finishing the query of a AD server, the AD Security Agent will send the updated user information to system.
User online time	Specifies the online duration of a user after successful SSO. After the user expires, it will be forced to log out. The range is 1 to 99 hours and the default value is 8 hours.
Client probing	
Enable WMI probing	Select the check box to enable WMI probing. • To enable WMI to probe the terminal PCs, the terminal

Option	Description
	PCs must open the RPC service and remote management. To enable the RPC service, you need to enter the **Control Panel >Administrative Tools> Services** and open the Remote Procedure Call and Remote Procedure Call Locator; to enable the remote management, you need to run the command prompt window (cmd) as administrator and enter the command **netsh firewall set service RemoteAdmin**. • WMI probing is an auxiliary method for security log monitor. which will probe all IPs in Discovered Users list. When the probed domain name does not match with the stored name, the stored name will be replaced by the probed name.
Probing Frequency	Specifies the interval of active probing action. The range is 1 to 99 minutes and the default value is 20 minutes.
User Send Delay	Specifies the delay time for a user to send messages. After configuring role mapping rules in the firewall, this function can prevent role mapping failures caused by the client users going online too quickly. The range is 0 to 999 ms and the default value is 0 ms.

5. On the <Discovered Server> tab, click **Auto Discover** to start automatic scanning the AD servers in the domain. Besides, you can click **Add** to input IP address of server to add it manually.

When querying event logs in multiple AD servers, the query order is from top to bottom in the list.

6. On the <Filtered User> tab, type the user name need to be filtered into the **Filtered user** text box. Click **Add**, and the user will be displayed in the Filtered User list. You can configure 100 filtered users, which are not case sensitive.

7. Click the <Discovered User> tab to view the corresponding relationship between the user name and user address that has been detected. Enter the user name and/or IP address/IP address + mask to search for users. conditions.

   Tip: The user added into the Filtered User list will not be displayed in the Discovered User list.

8. On the <AD Scripting> tab, click **Get AD Scripting** to get the script "Logonscript.exe". (For introduction and installation of this script, refer to "Using AD Scripting for SSO" on Page 496) .

9. Click **Commit** to submit all settings and start AD Security Agent service in the mean time.



Notes: After you have committed, AD Agent service will be running in the background all the time. If you want to modify settings, you can edit in the **AD Agent Configuration Tool** and click **Commit**. The new settings can take effect immediately.

Step 2: Configuring AD server for StoneOS

To ensure that the AD Security Agent can communicate with StoneOS, take the following steps to configure the AD server:

1. Click **Object >AAA Server** to enter the AAA server page.

2. Choose one of the following two methods to enter the Active Directory server configuration page:

- Click the New button on the upper left corner of the page, and choose **Active Directory Server** in the drop-down list.
- Choose the configured AD server and click the Edit button on the upper left corner of the page.

3. For basic configuration of AD server, see Configuraing Active Directory Server.
4. Click **OK** to finish the related configuration of AD server.

Step 3: Enabling and Configuring SSO Monitor

To connect SSO Monitor to AD Agent, take the following steps:

1. Click **Object** > **SSO Client** > **SSO Monitor**.
2. Click **New**. On the **SSO Monitor Configuration** page, take note of the following items:
   a. Server Address 1: The server address needs to be the IP address of the device where AD Agent software resides;
   b. Port: The port needs to be the same as that configured in AD Agent software;
   c. AAA Server: The server needs to be the AD server configured in Step 2;
   d. Organization Source: The source needs to be AAA Server. Force Timeout: We do not recommend that you configure this timeout and the timeout on AD Agent at the same time.
   For more information, see Using SSO Monitor for SSO.
3. Click **OK**.

After completing the above two steps, when domain user logs in the AD server, the AD Security Agent will send the user name, address and online time to the StoneOS and generates an authenticated user on the firewall.

Using TS Agent for SSO

The configurations of TS Agent for SSO include:

- Configuring the TS Agent server: Installing and running Hillstone Terminal Service Agent in Windows server.
- Configuring the TS Agent client: Configuring TS Agent parameters in StoneOS.

Step 1: Installing and running Hillstone Terminal Service Agent in Windows server

1. Click http://swupdate.hillstonenet.com:1337/sslvpn/download?os=windows-tsagent to download a Hillstone Terminal Service Agent installation program, and copy it to the Windows server.

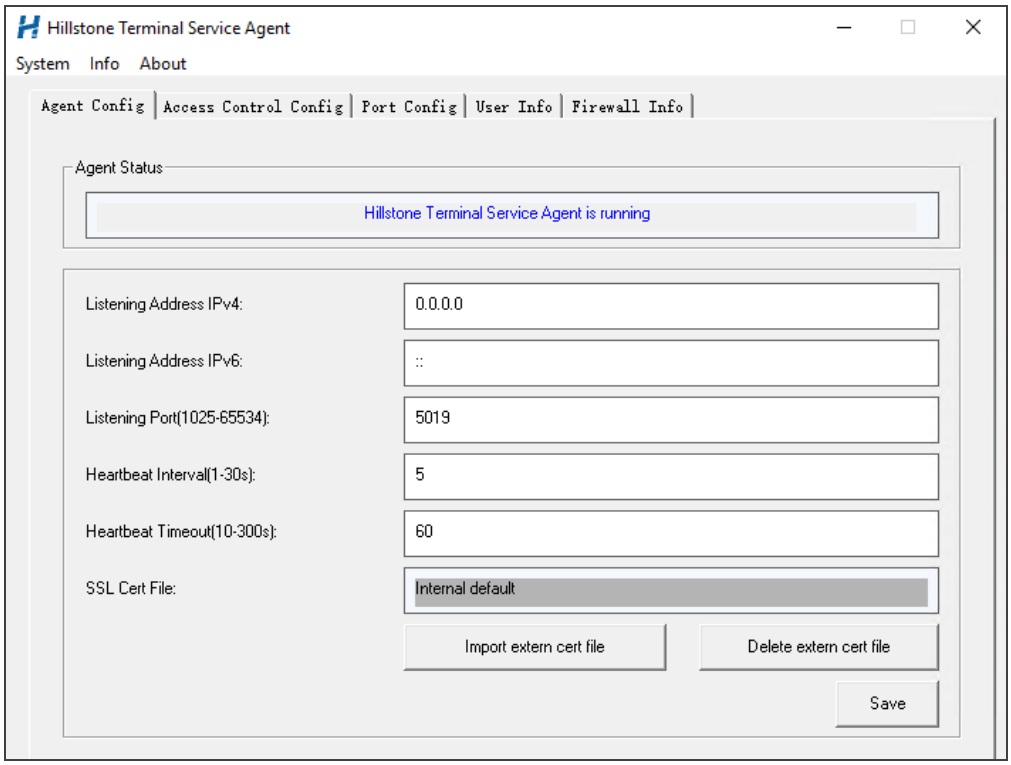
   

   Notes:

   - Windows Server 2008 R2, Windows Server 2016, and Windows Server 2019 are currently supported. Windows Server 2008 R2 Service Pack 1 and KB3033929 must be installed if Windows Server 2008 R2 is used.
   - It's recommended to close the anti-virus software before installing Hillstone Terminal Service Agent in Windows server.

2. Double-click HSTSAgent.exe to open it and follow the installation wizard to install it.
3. Start Hillstone Terminal Service Agent through one of the two following methods:
   - Double-click the Hillstone Terminal Service Agent shortcut on the desktop.
   - Click **Start** menu, and select **All app > Hillstone Terminal Service Agent**.

4. Click the **Agent Config** tab.

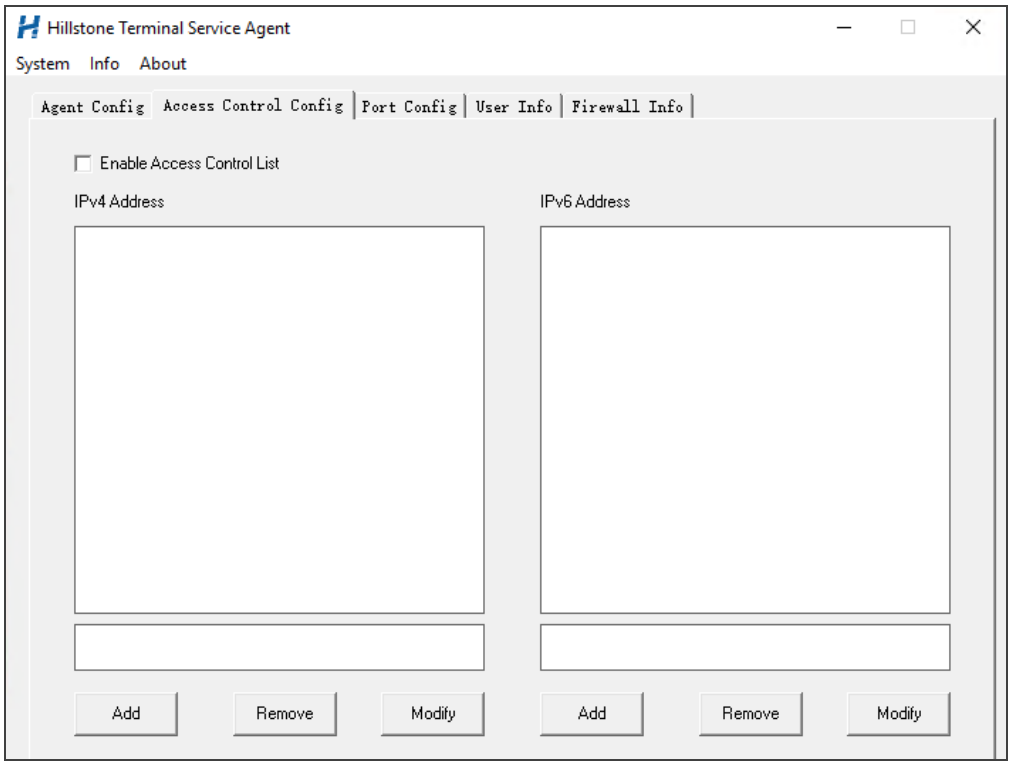


In the Agent Config tab, configure the following options.

Option	Description
Agent Status	Shows Hillstone Terminal Service Agent running status.
Listening Address IPv4	Specifies the IPv4 address to be listened. The default value is 0.0.0.0, which means listening all the IPv4 addresses.
Listening Address IPv6	Specifies the IPv6 address to be listened. The default value is ::, which means listening all the IPv6 addresses.
Listening Port	Specifies the listening port number. The range is 1025 to 65534. The default value is 5019. This port must be the same with the TS Agent server port configured in StoneOS, otherwise, the TS Agent client and the TS Agent server cannot communicate with

Option	Description
	each other.
Heartbeat Interval	Specifies the interval of sending heartbeat from the TS Agent client to the TS Agent server. The range is 1 to 30 seconds. The default value is 5 seconds.
Heartbeat Timeout	The TS Agent client will disconnect with the TS Agent server if it doesn't receive the heartbeat response from the server within the configured time. The range is 10 to 300 seconds. The default value is 60 seconds.
SSL Cert File	The TS Agent client synchronizes information with the TS Agent server through SSL connection. You can use the internal default SSL cert file or import external SSL cert file.
Import extern cert file	Click this button to import a new SSL cert file through the <Import extern cert file> dialog box. The encryption standard of the imported cert is PKCS12. The file is in .pfx format. To import the external cert file, you should create a PKI trust domain and import the CA certificate.
Delete extern cert file	Click this button to delete the external SSL cert file. After deletion, you need to restart the Hillstone Terminal Service Agent to make the default SSL cert file take effect. To restart the Hillstone Terminal Service Agent, click **Restart Agent Server** from the **System** drop-down menu.

5. Click the **Access Control Config** tab.

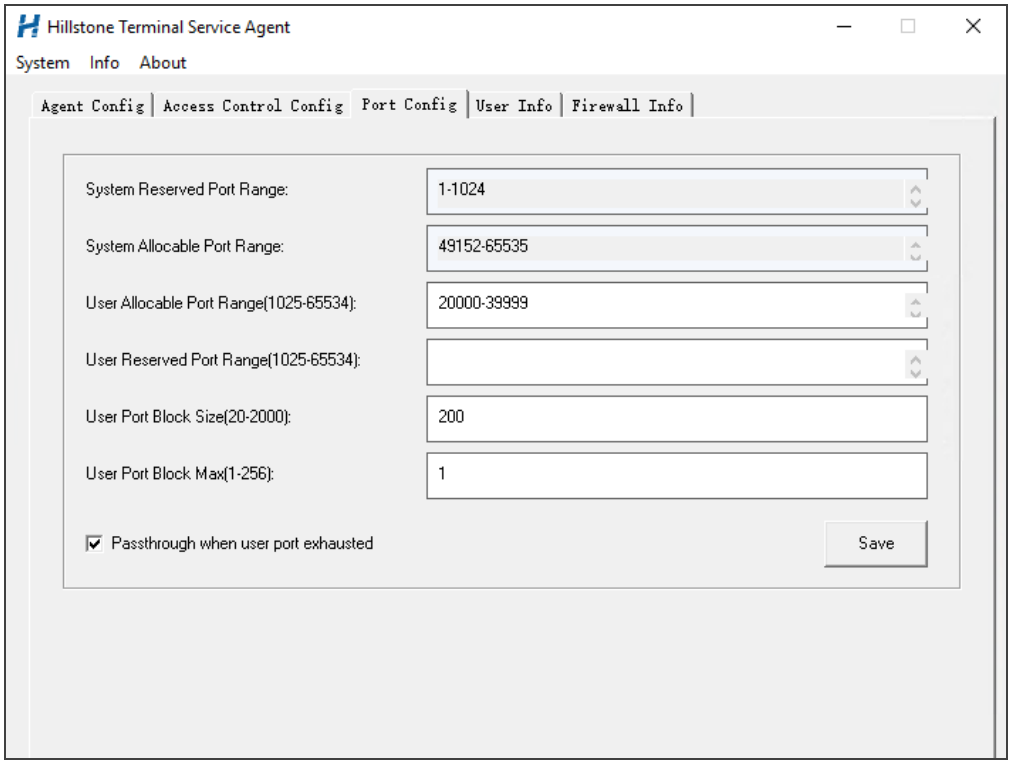


In the Access Control Config tab, configure the following options.

Option	Description
Enable Access Control List	Select this check box to check if the newly accessed IP address of StoneOS is in the IPv4 address list or IPv6 address list below, if not, the access will be denied. This function is disabled by default.
IPv4 Address	When the access control list feature is enabled, IPv4 addresses that are not in the list will be access denied.
IPv6 Address	When the access control list feature is enabled, IPv6 addresses that are not in the list will be access denied.
Add	Enter an IP address in the text box above **Add**, and clicks **Add**

Option	Description
	to add the IP address into the IPv4 addresses list or IPv6 addresses list.
Remove	Select an IP address in the IPv4 addresses list or IPv6 addresses list, and clicks **Remove** to delete the IP address from the list.
Modify	Select an IP address in the IPv4 addresses list or IPv6 addresses list, modifies the address in the text box below, and then clicks **Modify** to add the address into the list.

6. Click the **Port Config** tab.

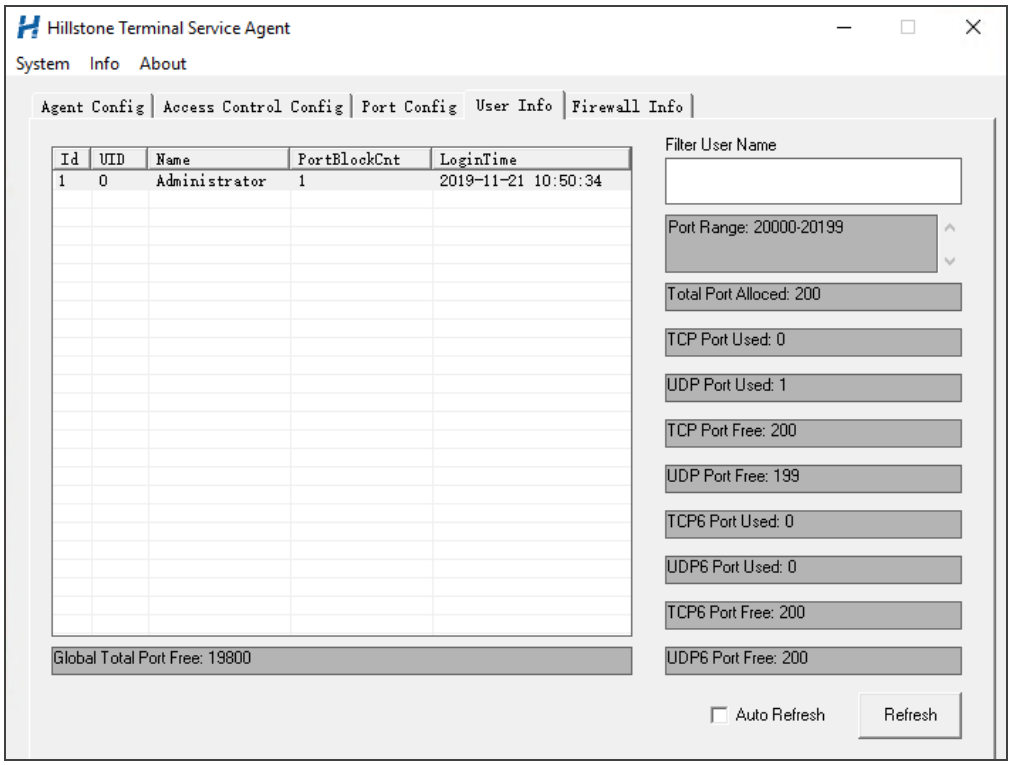


In the Port Config tab, configure the following options.

Option	Description
System	The range of ports reserved by the system, which is read from

Option	Description
Reserved Port Range	the system registry and cannot be modified.
System Allocable Port Range	The range of ports used by the system to dynamically allocate to users, which is read from the system registry and cannot be modified.
User Allocable Port Range	The total port range that can be allocated to the users. The range is 1025 to 65534. The default value is from 20000 to 39999. Only one port range can be configured each time, the minimum range size is the specified user port block size, and the maximum range size is 40960.
User Reserved Port Range	The user-defined reserved range of ports. The range is 1025 to 65534. The default value is NULL. You can configure more than one port ranges with each separated by a comma, such as 2000-3000,3500,4000-4200.
User Port Block Size	The number of ports allocated to the user each time. The range is 20 to 2000. The default value is 200.
User Port Block Max	The maximum number of port blocks allocated to each user. The range is 1 to 256. The default value is 1.
Passthrough when user port exhausted	Select the check box, and when the ports in the User Allocable Port Range are exhausted, system will allocate ports to users from the System Allocable Port Range. This option is checked by default.

7. Click the **User info** tab.

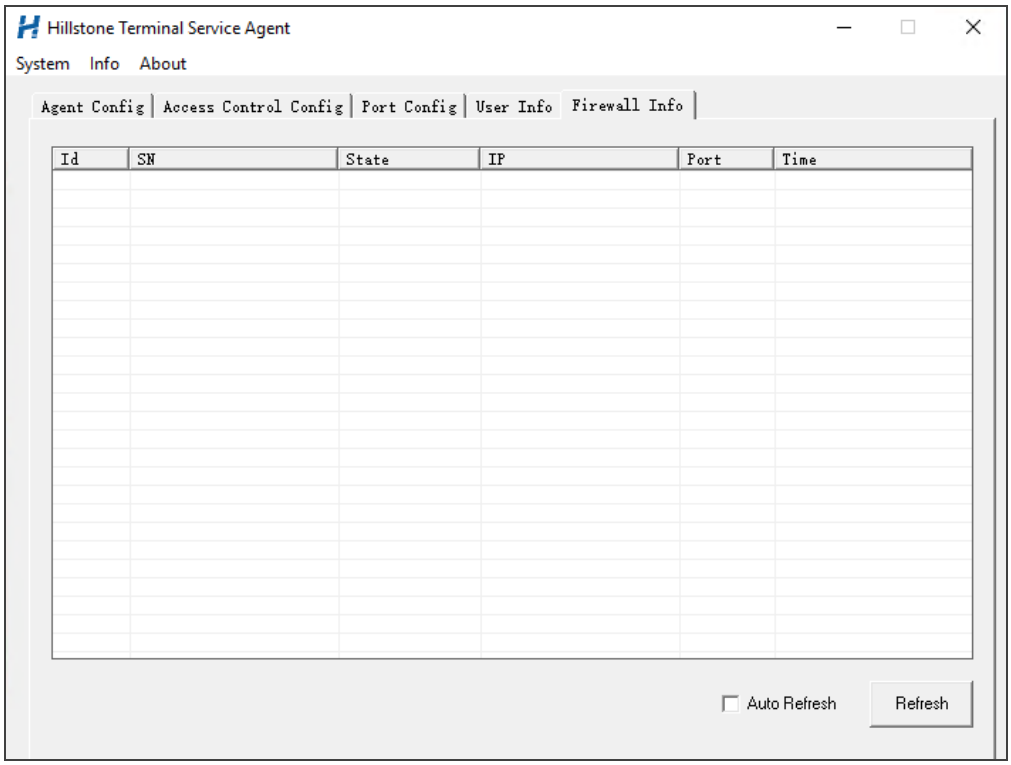


In the User Info tab, view information about users.

Option	Description
User Info. List	Shows the login user information, including ID, UID, user name, port block count and the login time. When users log in the TS Agent server using remote desktop services, Hillstone Terminal Service Agent will record the user info. in the list. It can record up to 2000 users info.
Filter User Name	Enter the user name in the text field, and click Refresh, the searched user info. will be displayed in the user info. list. The user name is case sensitive.

Option	Description
Global Total Port Free	The number of remaining ports available to the users.
Port Range	The port range already allocated to login users. After the user logs off, the system reclaims all the port ranges allocated to this user.
Total Port Alloced	Total number of ports allocated to the login users.
TCP/UDP/TCP6/UDP6 Port Used	The number of ports already used by users. After the user's connection to the Internet is disconnected, the system reclaims the ports.
TCP/UDP/TCP6/UDP6 Port Free	The number of ports available to the user when creating a new connection
Auto Refresh	Check the check box, the port statistics will be refreshed every 5 seconds.

8. Click the **Firewall Info** tab.



In the Firewall Info tab, view information about StoneOS.

Option	Description
Connected Device List	Displays StoneOS info. currently connected to TS Agent server, including ID, SN, connected status, IP address, port and time.
Auto Refresh	Check the check box, information of the connected devices will be refreshed every 5 seconds.

9. Configure related functions and view information using the Menu bar.

Menu bar options introduction.

System	
Restart agent server	Click this option to restart Hillstone Terminal Service Agent. When Hillstone Terminal Service Agent is being restarted,

System	
	Agent Status on the **Agent Config** tab shows "Hillstone Terminal Service Agent is stopped". When the restart is completed, **Agent Status** on the **Agent Config** tab shows "Hillstone Terminal Service Agent is running".
Info	
Open log info	Click this option, you can perform following operations in the pop-up Log Info dialog box: • Check one or more check boxes in the Info Select section, corresponding logs will be displayed in the log info list. • Select a log in the log info list, the complete info. of this log will be displayed in the text box at the lower left corner. • Type the character string in the **Filter** text box, and click **Refresh**, the log info. containing the character string will be displayed in the log info list. • Check the ID of one ore more logs in the log info. list, and click **Delete** to delete selected logs. • Click **Export to text** to export the log info. as a text file. • Click and drag the scroll slider at the lower left corner left or right to scroll through the log info. page quickly. The text field below displays the total number of log inform-

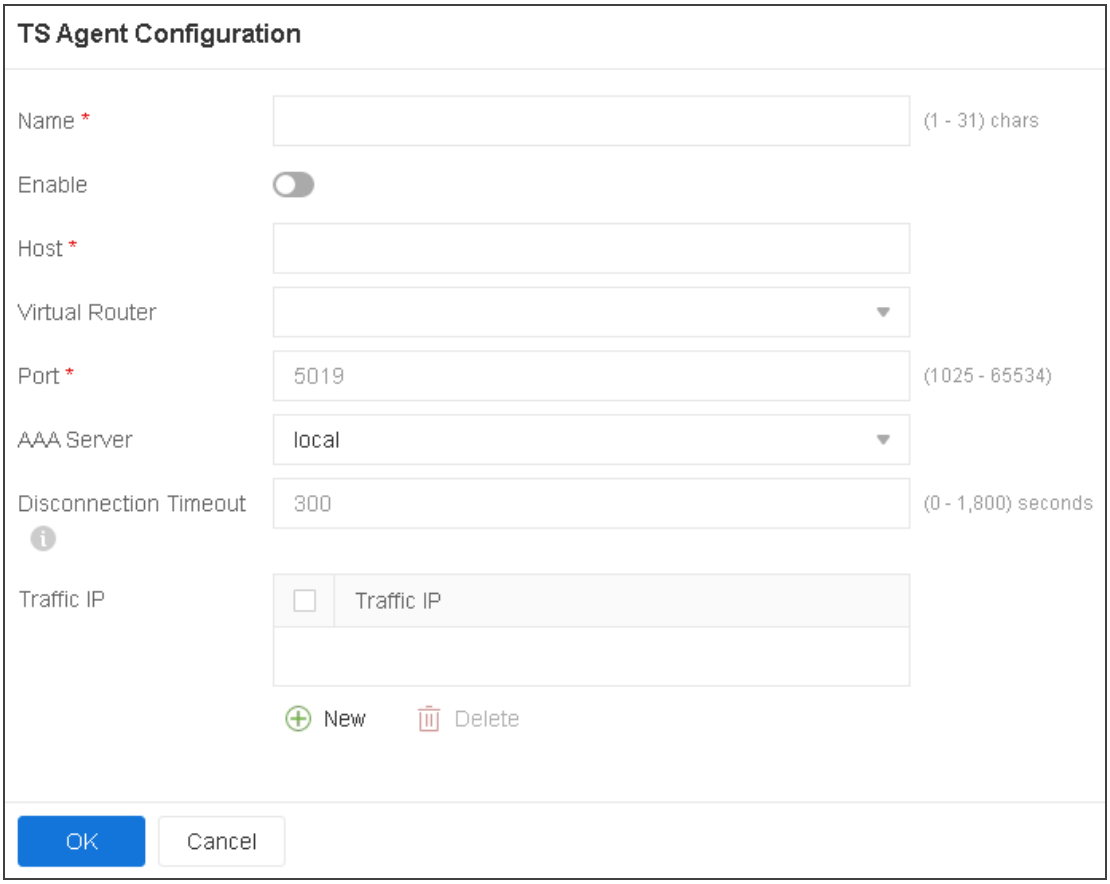
System	
	ation, the total number of log information pages, and the current page.
Log enable set	Click this option, and check or uncheck the type of log info., system will record or not record corresponding type of log info. The system record the Event, Alarm and Config log info. by default.
Open debug info	Click this option, the SMP (Service Process Module) debug info. file and the KM (Kernel Module) debug info. file display in the pop-up Debug Info dialog box. You can perform following operations: • Double-click the file name to open the file. • Select the file name, and press the Delete key on your key-board to delete the file.
SPM debug level set	Click this option, and check the level of the SMP debug info., system will record the info. at or above the selected level. The default level is Event. You can view the SMP debug info. in the Debug Info dialog box: the SMP debug info. at Critical and Error level display in the SPM error section; the SMP debug info. at other levels display in the SPM info section.
KM debug level set	Click this option, and check the level of the KM debug info., system will record the info. at or above the selected level. The default level is Critical. You can view the KM debug info. in the Debug Info dialog box: the KM debug info. at Critical and Error level display in the KM error section; the KM debug info. at

System	
	other levels display in the KM info section.
About	
About	Displays the information of version, copyright, etc.

Step 2: Configuring TS Agent parameters in StoneOS

To configure the TS Agent parameters in StoneOS, take the following steps:

1. Select **Object > SSO Client > TS Agent**.
2. Click **New**.



Option	Description
Name	Specifies the name of the new TS Agent. The range is 1 to 31 characters.
Status	Select **Enable** button to enable the TS Agent function. After enabling, StoneOS will establish SSL connection with the TS Agent server, as well as obtain user and port range information. System will also update the mapping information of traffic IPs, port ranges and user names in real time for online users.
Host	Specifies the management address of the TS Agent server. It can be a domain name, or an IPv4 or IPv6 address.
Virtual Router	Select the virtual router that the TS Agent server belongs to in the drop-down list.
Port	Specifies the port number of the TS Agent server. The default number is 5019. The range is 1025 to 65534. This port number must be the same with the listening port number of Hillstone Terminal Service Agent, otherwise, the TS Agent client and the TS Agent server cannot communicate with each other.
AAA Server	Select the referenced AAA server in the drop-down list. You can select the configured Local, AD or LDAP server, see "AAA Server" on Page 912. After selecting the AAA server, system can query the corresponding user group and role information of the online user on the referenced AAA server, so as to realize the policy control based on the user group and role.
Disconnection Timeout	When StoneOS disconnects with the TS Agent server, system will wait during the disconnection timeout. If system still fails

Option	Description
	to connect within the configured time, it will delete online user. The range is 0 to 1800 seconds. The default value is 300. 0 means delete the online user immediately.
Traffic IP	Specifies the traffic IP address, that is the network interface IP address of the TS Agent server. It cab be an IPv4 or IPv6 address. You can specify up to 4 IP addresses. Enter an IP address in the text field, and click **Add** to add the IP address into the Traffic IP list below. Check an IP address in the Traffic IP list, and click **Delete** to delete the IP address.

3. Click **OK** to finish the configuration of TS Agent.

After all the above configurations are finished, when users log in the TS Agent server using remote desktop services, the Hillstone Terminal Service Agent will allocate port ranges to users and send the port ranges and users information to the system. At the same time, the system will create the mappings of traffic IPs, port ranges and users.

802.1x

802.1X is a standard defined by IEEE for Port-based Network Access Control. It uses Layer-2 based authentication (protocol: EAPOL, Extensible Authentication Protocol over LAN) to verify the legality of the users accessing the network through LAN. Before authentication, the security device only allows the 802.1X message to pass through the port. After authentication, all of the normal traffic can pass through.

The AAA servers for 802.1x are Local server and Radius server. Other types of AAA servers like AD or LDAP server do not support 802.1x.

The authenticating process is the same with other authentication, please refer to "Chapter 7 Authentication" on Page 469.

Configuring 802.1x

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

A complete configuration for 802.1x authentication includes the following points:

- Prerequisite: Before configuration, you should already have the AAA server you want (only local or Radius server is supported for 802.1x). The AAA server has been added in the fire-wall system (refer to AAA server), and the interface or VLAN for authentication has been bound to a security zone (refer to interface or VLAN).
- Configuration key steps:
    1. Creating a 802.1x profile.
    2. Creating a security policy to allow accessing.
- In the user's PC, modify the network adapter's properties: If the computer is connected to the 802.1x interface, this computer should enable its authentication function on its LAN port (right click **LAN** and select **Properties**, in the prompt, under the <Authentication> tab, select **MD5-Challenge** or **Microsoft: Protected EAP (PEAP)**, and click **OK** to confirm.)



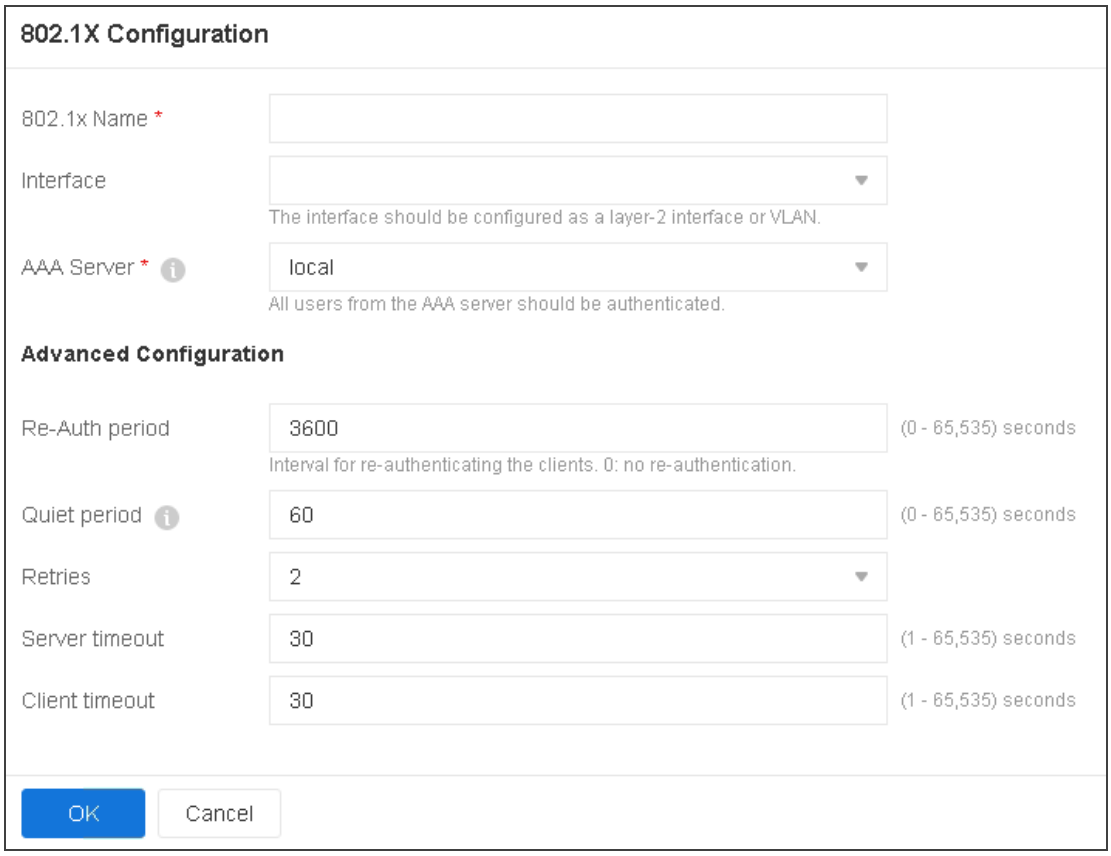
Notes: Early versions of Windows have enabled 802.1x by default, but Windows 7 and Window 8 do not have this feature enabled. To enable 802.1x, please search online for a solution that suits your system.

Creating 802.1x Profile

To create a 802.1x profile, take the following steps:

1. Select **Network > 802.1X > 802.1X**.

2. Click **New** and a prompt appears.



Under the Basic tab and Advanced tab, enter values.

Basic Configuration	
802.1x Name	Enter a name for the 802.1x profile
Interface	Select the interface for 802.1x authentication. It should be a Layer-2 interface or a VLAN interface.
AAA Server	Select the AAA server for 802.1x authentication. It should be a local server or a Radius server.
Access	Select an access mode. If you select **Port** and one of the

Basic Configuration	
Mode	clients connected to 802.1x interface has passed authentication, all clients can access the Internet. If you select **MAC**, every client must pass authentication before using Internet.
Advanced Configuration	
Port authorized	If you select Auto, system will allow users who have successfully passed authentication to connect to network; If you select Force-unauthorized, system will disable the authorization of the port; as a result, no client can connect to the port, so there is no way to connect to the network.
Re-auth period	Enter a time period as the re-authentication time. After a user has successfully connected to the network, system will automatically re-auth the user's credentials. The range is from 0 to 65535 seconds. If the value is set to 0, this function is disabled.
Quiet period	If the authentication fails, it will take a moment before system can process the authenticating request from the same client again. The range is 0 to 65535 seconds, and the default value is 60 seconds. If this value is set to 0, system will not wait, and will immediately process the request from the same client.
Retries	After sending an authentication request to the client and receives a response containing the expected data, the

Basic Configuration	
	authenticator transmits the client's response data to the authentication server and waits for a response. If the authentication server does not answer, the authenticator will resend an authentication request to the client until receiving a response from the authentication server or exceeding the allowed maximum retry times. The range is 1 to 10 times, and the default is 2 times.
Sever timeout	After sending an authentication request to the client and receives a response containing the expected data, the authenticator transmits the client's response data to the authentication server and waits for a response. If the server does not answer the authenticator within a specified time, the authenticator will resend an authentication request to the client. The range is 1 to 65535 seconds, the default value is 30 seconds.
Client timeout	When the authenticator sends a request to ask the client to submit his/her username, the client needs to respond within a specified period. If the client does not respond before timeout, system will resend the authentication request message. The range is 1 to 65535 seconds, and the default value is 30 seconds.

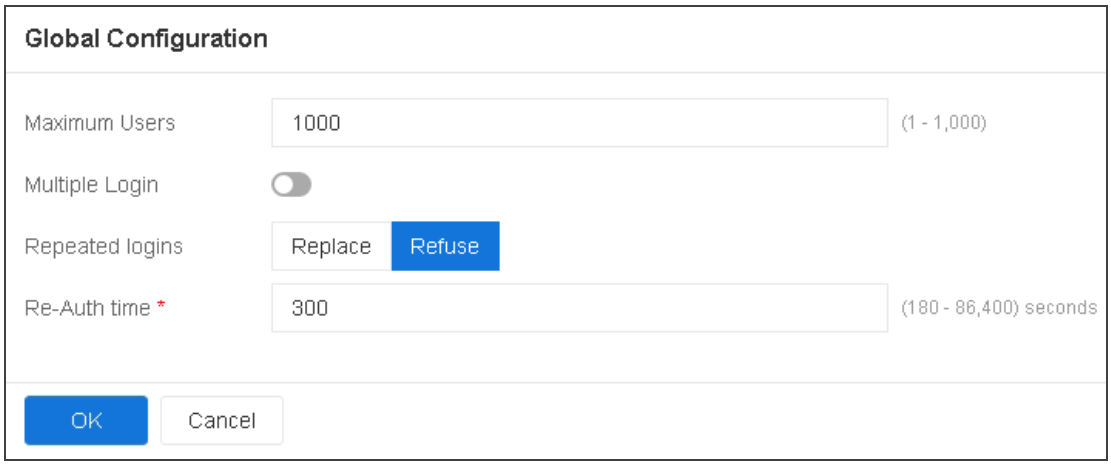
3. Click **OK**.

802.1x Global Configuration

Global parameters apply to all 802.1x profiles.

To configure global parameters, take the following steps:

1. Select **Network > 802.1X > Global Configuration**.



Option	Description
Maximum Users	The maximum user client number for a authentication port.
Multiple logins	You may choose to allow or disable one account to login from different clients. • **Disable**: If you select Disable, one account can only login from one client simultaneously. Then, when you want to kick off the old login user, you should select **Replace**; if you want to disallow new login user, select **Refuse**. • **Enable**: If you select **Enable**, different clients can use one account to login. If you do not limit the login client number, select **Unlimited**; if you want to set up a maximum login number, select **Max attempts** and enter a value for maximum user client

Option	Description
	number.
Re-Auth time	Specify a time for authentication timeout value. If the client does not respond within the timeout period, the client will be required to re-enter its credentials. The range is 180 to 86400 seconds, the default value is 300 seconds.

2. Click **OK**.

Viewing Online Users

To view which authenticated users are online:

1. Select **Network > 802.1X > Online user**.
2. The page will show all online users. You can set up filters to view results that match your conditions.

PKI

PKI (Public Key Infrastructure) is a system that provides public key encryption and digital signature service. PKI is designed to automate secret key and certificate management, and assure the confidentiality, integrity and non-repudiation of data transmitted over the Internet. The certificate of PKI is managed by a public key by binding the public key with a respective user identity by a trusted third-party, thus authenticating the user over the Internet. A PKI system consists of Public Key Cryptography, CA (Certificate Authority), RA (Certificate Authority), Digital Certificate and related PKI storage library.

PKI terminology:

- Public Key Cryptography: A technology used to generate a key pair that consists of a public key and a private key. The public key is widely distributed, while the private key is only

known to the recipient. The two keys in the key pair complement each other, and the data encrypted by one key can only be decrypted by the other key of the key pair.

- CA: A trusted entity that issues digital certificates to individuals, computers or any other entities. CA accepts requests for certificates and verifies the information provided by the applicants based on certificate management policy. If the information is legal, CA will sign the certificates with its private key and issue them to the applicants.
- RA: The extension to CA. RA forwards requests for a certificate to CA, and also forwards the digital certificate and CRL issued by CA to directory servers in order to provide directory browsing and query services.
- CRL: Each certificate is designed with expiration. However, CA might revoke a certificate before the date of expiration due to key leakage, business termination or other reasons. Once a certificate is revoked, CA will issue a CRL to announce the certificate is invalid, and list the series number of the invalid certificate.

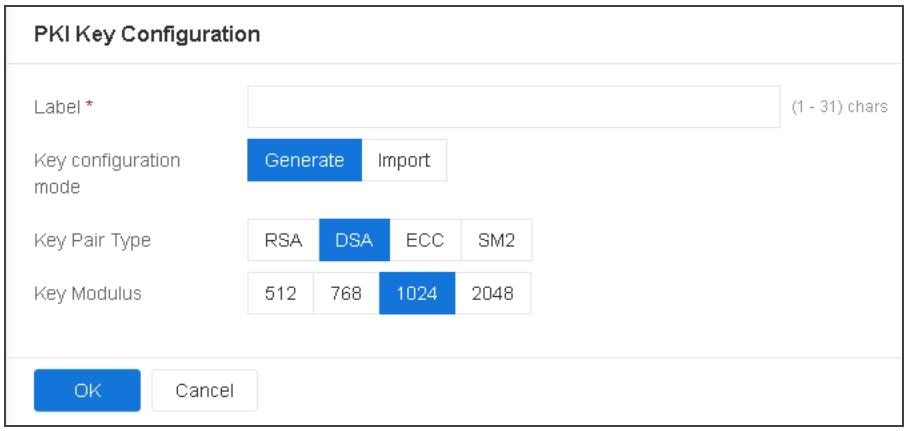
PKI is used in the following two situations:

- IKE VPN: PKI can be used by IKE VPN tunnel.
- HTTPS/SSH: PKI applies to the situation where a user accesses a Hillstone device over HTTPS or SSH.
- "Sandbox" on Page 1376: Support the verification for the trust certification of PE files.

Creating a PKI Key

1. Select **System > PKI > Key**.

2. Click **New**.



Option	Description
Label	Specifies the name of the PKI key. The name must be unique.
Key configuration mode	Specifies the generation mode of keys, which includes Generate and Import.
Key Pair Type	Specifies the type of key pair, either RSA, ECC, DSA or SM2.
Key Modulus	Specifies the modulus of the key pair. Valid values for modulus of RSA: 1024, 2048 (default), 512, 768, and 4096 bits. Valid values for modulus of DSA: 1024 (default), 2048, 512, and 768 bits, and the modulus of SM2 is 256.
EC group	Specifies the EC group of the key pair when you choose ECC. It includes P-256, P-384, P-521 elliptic curves. The default EC group is P-256.
Type	Specifies the type of key , including Encryption Key and Key

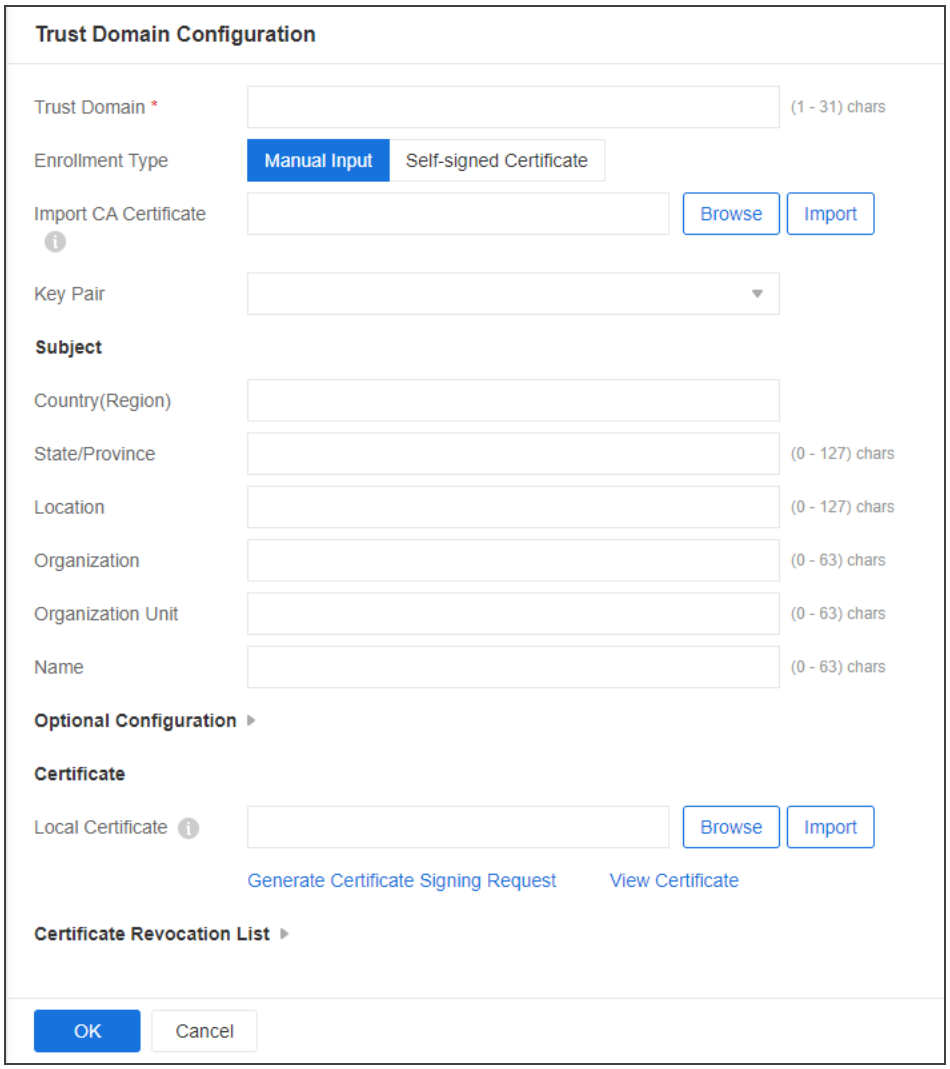
Option	Description
	Pair . • Encryption Key - Protects the signing key pair by digital envelope. If you select this option, you should specify the signing key pair when importing key. • Key Pair - If you select this option, you should specify the imported key pair type as RSA, DSA or SM2.
Import Key	Browse your local file system and import the key file.

3. Click **OK**.

Creating a Trust Domain

1. Select **System > PKI > Trust Domain**.

2. Click **New**.



In the Basic Configuration tab, configure values for basic properties.

Option	Description
Basic	
Trust Domain	Enter the name of the new trust domain.
Enrollment Type	Use one of the two following methods: • Select **Manual Input**, and click **Browse** to find the certificate and click **Import** to import it into system. • Select **Self-signed Certificate**, and the certificate will be generated by the device itself. **Notes:** • The system will check the validity of the imported certificate. "Subject Type=CA" needs to be included in the "Basic Constraints" field of the imported CA certificate. • The self-signed certificate generated will contain the "SSL client authentication" or "SSL server authentication" property.
Key Pair	Select a key pair.
Subject	
Name	Enter a name of the subject.
Country	Enter the name of applicant's country or region. Only an abbre-

Option	Description
Basic	
(Region)	viation of two letters are allowed, like CN.
Location	Optional. The location of the applicant.
State/Province	Optional. State or province name.
Organization	Optional. Organization name.
Organization Unit	Optional. Department name within applicant's organization.
Optional Configuration	
IP	Click **New** to specify the IP address to be added to the Subject Alternative Name list. Both IPv4 and IPv6 addresses are supported.
DNS Name	Click **New** to specify the DNS name to be added to the Subject Alternative Name list. The value range is from 1 to 255 characters.

3. Click **Generate Certificate Signing Request**, and a string of code will appear.



4. Copy this code and send it to CA via email.



5. When you receive the certificate sent from CA. Click **Browse** to import the certificate.



6. (Optional) In the CRL tadb, configure the following.

Certification Revocation List	
Check	• No Check - System does not check CRL. This is the default option. • Optional - System accepts certificating from peer, no matter if CRL is available or not. • Force - System only accepts certificating from peer when CRL is available.
URL 1-3	The URL address for receiving CRL. At most 3 URLs are allowed, and their priority is from 1 to 3. • Select **http://** if you want to get CRL via HTTP.

Certification Revocation List	
	• Select **ldap://** if you want to get CRL via LDAP. • If you use LDAP to receive CRL, you need to enter the login-DN of LDAP server and password. If no login-DN or password is added, the transmission will be anonymous.
Auto Update	Update frequency of CRL list.
Manually Update	Get the CRL immediately by clicking **Obtain CRL**.

7. Click **OK**.

Importing/Exporting Trust Domain

To simplify configurations, you can export certificates (CA or local) and private key (in the format of PKSC12) to a computer and import them to another device.

To export a PKI trust domain, take the following steps:

1. Select **System > PKI > Trust Domain Certificate**.
2. Select a domain from drop-down menu.
3. Select the radio button of the item you want to export, and click **Export**.
   If you choose PKCS, you need to set up password.
4. Click **OK**, and select a storage path to save the item.

To import the saved trust domain to another device, take the following steps:

1. Log in the other device, select **System > PKI > Trust Domain Certificate**.
2. Select a domain from drop-down menu.

3. Select the radio button of the item you want to import, and click **Import**.

   If you choose PKCS, you need to enter the password when it was exported.

4. Click **Browse** and find the file to import.

5. Click **OK**. The domain file is imported.

Importing Trust Certification

System will not detect the PE file whose certification is trusted. To import trust certification of PE files, take the following steps:

Configuring a Certificate Chain

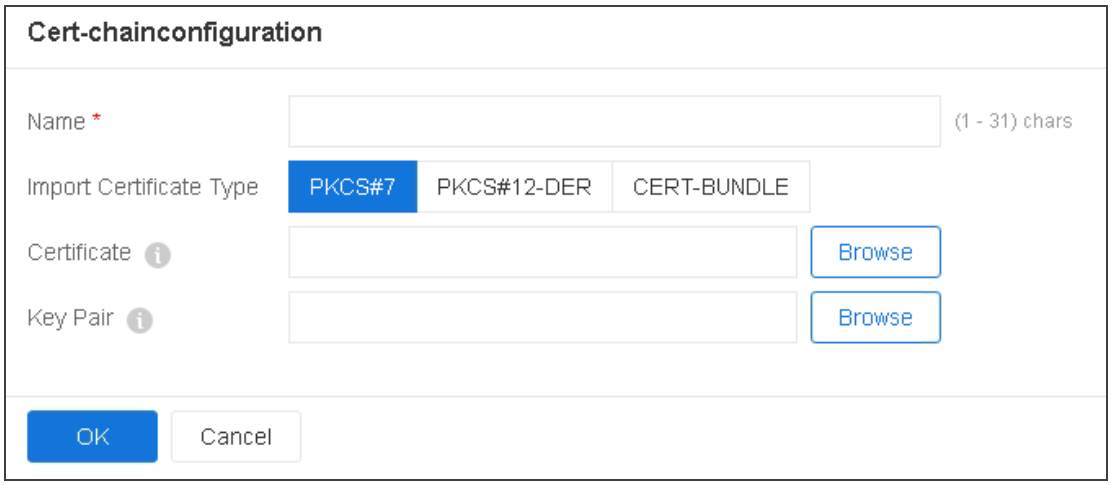
A certificate chain consists of a root CA certificate, any intermediate CA certificates, and a CA-signed user certificate. Browsers consider that the certificate of the current user is valid and trusted only of each certificate in the certificate chain is valid. A root CA certificate lies in the top most position of the chain of trust hierarchy. Intermediate certificates branch off root certificates like branches of trees. They act as middle-men between the protected root certificates and the server certificates issued out to the public. There will always be at least one intermediate certificate in a chain, but there can be more than one.

Creating a Certificate Chain

To create a certificate chain, take the following steps:

1. Select **System** > **PKI** > **Cert-chain**.

2. Click **New**.



Option	Description
Name	Specifies the name of the certificate chain, which can be 1 to 31 characters.
Import Certificate Type	Specifies the format of the certificate chain. Valid values: PKCS#7, PKCS#12, and CERT-BUNDLE. CERT-BUNDLE indicates PEM-formatted certificate chains.
Password	For certificate chains in the PKCS#12 format, you need to specify the password that is used for decryption.
Certificate	Click **Browse** and select a certificate chain file that you want to import from your PC. A certificate chain can contain at most 6 certificates. These certificates need to be able to complete a chain but there is no limitation on the order of these certificates.
Key Pair	If the type of the certificate chain is PKCS#7 or CERT-BUNDLE, you can import the private key of the last-level certificate used for encryption and decryption. Click **Browse** and

Option	Description
	select a private key file that you want to import from your PC.

3. Click **OK**.

Exporting a Certificate Chain

To export a certificate chain to your PC, take the following steps:

1. Select **System** > **PKI** > **Cert-chain**.
2. Select a certificate chain from the list.
3. Click **Export Cert-chain**. If the certificate chain is in the PKCS#12 format, you need to enter a password.

Configuring Certificate Validity Check

By default, the system sends an alarm per day a week before the certificate expires. When the certificate expires, the system records an event log at critical level.

To configure certificate validity check, take the following steps:

1. Select **System** > **PKI** > **Validity Check**.

   On the Validity Check page, configure the following options:

Option	Description
Validity Check	Turn on the switch to enable certificate validity check. By default, this function is enabled.
Validity Check Interval	Specifies the interval at which certificate validity is checked. Valid values: 1 to 100, in hours. Default value: 24.

Option	Description
The Pre-warning Time	Specifies the warning days before certificate expiration. Valid values: 1 to 1000, in hours. Default value: 168.

2. Click **OK**.

Online Users

To view the online authenticated users, take the following steps:

1. Select **Network >WebAuth > Online Users**.
2. The page will show all online users. You can set up filters to views results that match your conditions.



- User Name: Displays the name of online users.
- IP/MAC: Displays the IP or MAC address of online users.
- Interface: Displays the authentication interface of online users.
- Online Time: Displays the online time of online users.
- Authentication Type: Displays the authentication type of online users.
- Operation: Displays the executable operation of online users.

Chapter 8 VPN

System supports the following VPN functions:

- "IPSec VPN" on Page 556: IPSec is a security framework defined by the Internet Engineering Task Force (IETF) for securing IP communications. It is a Layer 3 virtual private network (VPN) technology that transmits data in a secure tunnel established between two endpoints.
- "SSL VPN" on Page 605: SSL provides secure connection services for TCP-based application layer protocols by using data encryption, identity authentication, and integrity authentication mechanisms.
- "L2TP VPN" on Page 711: L2TP is one protocol for VPDN tunneling. VPDN technology uses a tunneling protocol to build secure VPNs for enterprises across public networks. Branch offices and traveling staff can remotely access the headquarters' Intranet resources through a virtual tunnel over public networks.
- "VXLAN" on Page 722:Virtual extensible local area network (VXLAN) is a tunnel encapsulation technology for large layer 2 network expansion overe NOV3 that uses MAC-in-UDP encapsulation. VXLAN uses a 24-bit network segment ID, called VXLAN network identifier (VNI), to identify users. This VNI is similar to a VLAN ID and supports a maximum of 16M [(2^24 - 1)/1024^2] VXLAN segments. VXLAN uses MAC-in-UDP encapsulation to extend Layer 2 networks to ensure uninterrupted services during VM migration, the IP address of the VM must remain unchanged.
- "GRE VPN" on Page 723: Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork. StoneOS uses GRE over IPSEC feature to ensure the security of routing information passing between networks.

IPSec VPN

IPSec is a widely used protocol suite for establishing a VPN tunnel. IPSec is not a single protocol, but a suite of protocols for securing IP communications. It includes Authentication Headers (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE) and some authentication methods and encryption algorithms. IPSec protocol defines how to choose the security protocols and algorithms, as well as the method for exchanging security keys among communicating peers, while offering the upper layer protocols with network security services, including access control, data source authentication, data encryption, etc.

Basic Concepts

- Security association
- Encapsulation modes
- Establishing SA
- Using IPSec VPN

Security Association (SA)

IPSec provides encrypted communication between two peers which are known as IPSec ISAKMP gateways. Security Association (SA) is the basis and essence of IPSec. SA defines some factors of communication peers like the protocols, operational modes, encryption algorithms (DES, 3DES, AES-128, AES-192 and AES-256), shared keys of data protection in particular flows and the life cycle of SA, etc.

SA is used to process data flow in one direction. Therefore, in a bi-directional communication between two peers, you need at least two security associations to protect the data flow in both of the directions.

Encapsulation Modes

IPSec supports the following IP packet encapsulation modes:

- Tunnel mode - IPSec protects the entire IP packet, including both the IP header and the payload. It uses the entire IP packet to calculate an AH or ESP header, and then encapsulates the original IP packet and the AH or ESP header with a new IP header. If you use ESP, an ESP trailer will also be encapsulated. Tunnel mode is typically used for protecting gateway-to-gateway communications.
- Transport mode - IPSec only protects the IP payload. It only uses the IP payload to calculate the AH or ESP header, and inserts the calculated header between the original IP header and payload. If you use ESP, an ESP trailer is also encapsulated. The transport mode is typically used for protecting host-to-host or host-to-gateway communications.

Establishing SA

There are two ways to establish SA: manual and IKE auto negotiation (ISAKMP).

- Manually configuring SA is complicated as all the information will be configured by yourself and some advanced features of IPSec are not supported (e.g. timed refreshing), but the advantage is that manually configured SA can independently fulfill IPSec features without relying on IKE. This method applies to a situation with a small number of devices or an environment of static IP addresses.
- IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining SA to the IKE auto negotiation function. This method is for medium and large dynamic networks. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates IPSec SA using the established ISAKMP. Establishing SA in two phases can speed up key exchanging.

Using IPSec VPN

To apply VPN tunnel feature in the device, you can use policy-based VPN or route-based VPN.

- Policy-based VPN - Applies the configured VPN tunnel to a policy so that the data flow which conforms to the policy settings can pass through the VPN tunnel.
- Route-based VPN - Binds the configured VPN tunnel to the tunnel interface and define the next hop of static route as the tunnel interface.

Configuring an IPSec VPN

IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining SA to the IKE auto negotiation function. This method is for medium and large dynamic network. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates IPSec SA using the established ISAKMP. Establishing SA in two phases can speed up key exchanging.

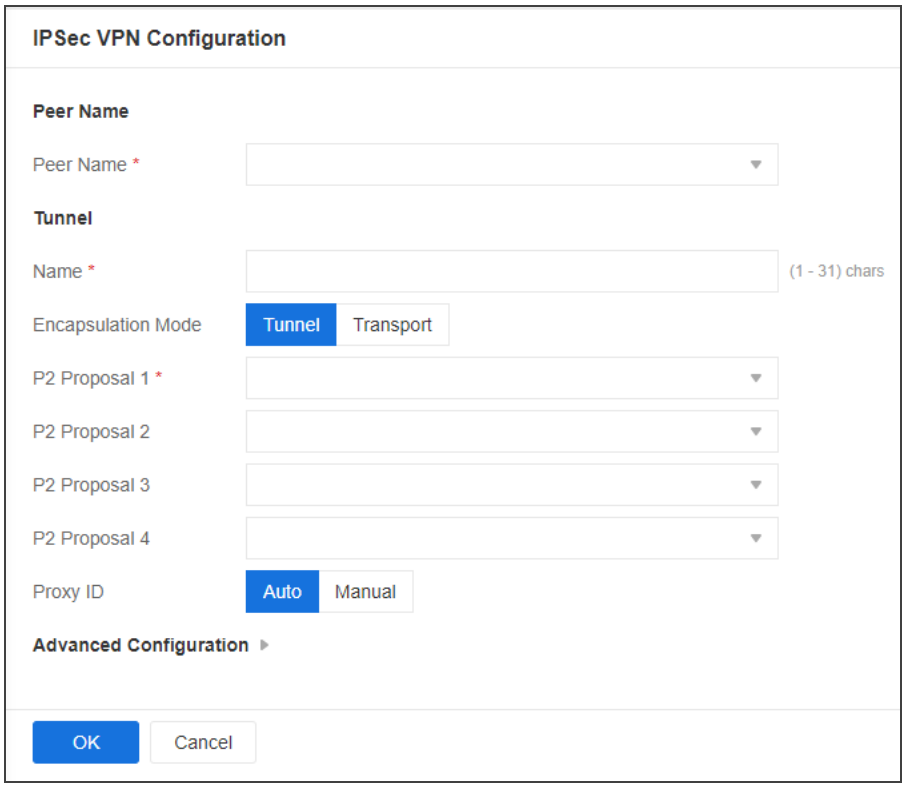
To configure an IPSec VPN, you need to confirm the Phase 1 proposal, the Phase 2 proposal, and the VPN peer. After confirming these three contents, you can proceed with the configuration of IKE VPN settings.

Configuring an IPSec VPN

To configure IPSec VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.

2. In the IPSec VPN tab, click **New**.



In the Peer Name tab, configure the corresponding options.

Peer	
Peer Name	Specifies the name of the ISAKMP gateway. To create an ISAKMP gateway, click ⊕. For detailed information, refer to Configuring a VPN Peer.

In the Tunnel tab, configure the corresponding options.

Tunnel	
Name	Type a name for the tunnel.
Encapsulation Mode	Specifies the encapsulation mode, including tunnel mode and transport mode. The default is tunnel mode.

Tunnel	
P2 Proposal 1/2/3/4	Specifies the P2 proposal for tunnel. To create a P2 proposal, click ⊕. You can define up to four P2 proposals for an ISAKMP gateway. For detailed information, refer to Configuring a Phase 2 Proposal.
Proxy ID	Users need to specify the IKE phase 2 ID to distribute and limit IPSec VPN traffic. Phase 2 ID consists of a local network segment, a remote network segment, and the service. During the configuration, you need to configure phase 2 IDS on the local and remote devices. Then, the local and remote devices negotiate to create an IKE IPSec tunnel. You can specify one or more phase 2 IDs to create one or more IKE IPSec tunnels. The system distributes and limits tunnel traffic according to the phase 2 ID of each tunnel. When using the IKEv2 protocol, only manual configuration of proxy IDs is supported. If you do not need to distribute or limit IPSec VPN traffic, you do not need to configure this parameter. For details about how to enable IPSec VPN traffic distribution and Limitation function, see Check ID. Specifies ID of Phase 2 for the tunnel which can be Auto or Manual. • Auto - The Phase 2 ID is automatically designated. • Manual - The Phase 2 ID is manually designated. Manual configuration of P2 ID includes the following options: • Local IP/Netmask - Specifies the IP/ mask of the local network segment in phase 2.

Tunnel	
	• Remote IP/Netmask - Specifies the IP/ mask of the remote network segment(peer device) in phase 2. • Service - Specifies the service or protocol name of the traffic that can be transmitted by IKE IPSec tunnels in phase 2. **Note**: By default, the Phase 2 IDs of the local and peer device need to be configured accordingly. If the IDs configured on the two device cannot match, the negotiation will fail. In this case, if you enable the Accepting All Proxy ID function on the responder's device, the negotiation succeeds. For details about how to enable **Accepting All Proxy ID** function, see Accepting All Proxy ID

3. If necessary, click the **Advanced Configuration** tab to configure some advanced options.

In the Advanced Configuration tab, configure the corresponding options.

Advanced	
Commit Bit	Select the **Enable** check box to make the corresponding party configure the commit bit function, which can avoid packet loss and time difference. However, commit bit may slow the responding speed.
Auto Connect	Select the **Enable** check box to enable the auto connection function. By default, this function is disabled. The device has two methods of establishing SA: auto and intrigued traffic mode. When it is auto mode, the device will check SA status every 60 seconds and initiate negotiation request when SA is not established; when it is in intrigued traffic mode, the tun-

Advanced	
	nel will send negotiation request only when there is traffic passing through the tunnel. By default, the intrigued traffic mode is enabled. **Note**: Auto connection works only when the peer IP is static and the local device is the initiator.
Accept-all-proxy-ID	This function needs to be configured on the responder device of IKE tunnel negotiation. After it is enabled, the responder device will accept the second-phase ID configured by the peer (negotiation initiator) and set its phase 2 ID according to the peer. In this way, the two ends of the IKE tunnel can successfully negotiate. This function is often used in scenarios where the responder device cannot perceive or is not interested in the initiator's Phase 2 ID. **Note**: When multiple Phase 2 IDs are configured on the responder device (that is, multiple IKE tunnels are configured), you need to disable this function. Otherwise, only one tunnel can be negotiated.
Enable Idle Time	Select the **Enable** check box to enable the idle time function. By default, this function is disabled. This time length is the longest time the tunnel can exist without traffic passing through. When the time is over, SA will be cleared.
DF-Bit	Select the check box to allow the forwarding device to execute IP packet fragmentation. The options are: • Copy - Copies the IP packet DF options from the sender directly. This is the default value. • Clear - Allows the device to execute packet fragmentation.

Advanced	
	• Set - Disallows the device to execute packet fragmentation.
Anti-Replay	Anti-replay is used to prevent hackers from attacking the device by resending the sniffed packets, i.e., the receiver rejects the obsolete or repeated packets. By default, this function is disabled. • Disable - Disables this function. • 32 -Specifies the anti-replay window as 32. • 64 - Specifies the anti-replay window as 64. • 128 - Specifies the anti-replay window as 128. • 256 - Specifies the anti-replay window as 256. • 512 - Specifies the anti-replay window as 512.
UDP Checksum	Click the checkbox to enable/disable calculating the checksum of UDP packet. By default, this function is disabled.
Check ID	Select the **Enable** check box to enable the check ID function(distribute or limit the IPsec VPN traffic). By default, this function is disabled. Before configuring, ensure that the phase 2 ID has been configured and phase 2 negotiations has been successful. After this function is enabled, the device filters the inbound and outbound traffic of the IKE tunnel according to phase 2 ID and then distributes and limits the inbound and outbound traffic. Traffic that does not match phase 2 IDs is discarded. Details are as follows:

Advanced	
	• **Distribution**: Based on the configuration of Phase 2 IDs, the traffic distribution function can distribute the traffic at the IKE tunnel ingress interface when the traffic flow into the IKE tunnel. If the elements of source IP address, destination IP address, and the type of the traffic can match the configuration of a certain Phase 2 ID, this kind of traffic will flow into the corresponding IKE tunnel for encapsulation and sending. If the traffic cannot match any Phase 2 IDs, it will be dropped. • **Limitation**: Based on the configuration of Phase 2 IDs, the traffic limitation function can limit the traffic at the IKE tunnel egress interface when the traffic flows out of the IKE tunnel. After the traffic was de-encapsulated, StoneOS checks the elements of source IP address, destination IP address, and the type of the traffic to see whether this kind of traffic matches a certain Phase 2 ID or not. If matched, the traffic will be dealt with. If not matched, the traffic will be dropped.
Tunnel State Notify	Select the **Enable** check box to enable the tunnel state notification function. With this function enabled, for route-based VPN, system will inform the routing module about the information of the disconnected VPN tunnel and update the tunnel route once any VPN tunnel disconnection is detected; for policy-based VPN, system will inform the policy module about the information of the disconnected VPN tunnel and update the tunnel policy once any VPN tunnel disconnection is detected.

Advanced	
VPN Track	Select the **Enable** check box to enable the VPN track function. The device can monitor the connectivity status of the specified VPN tunnel, and also allows backup or load sharing between two or more VPN tunnels. This function is applicable to both route-based and policy-based VPNs. The options are: • Track Interval - Specifies the interval of sending Ping packets. The unit is second. • Threshold - Specifies the threshold for determining the track failure. If system did not receive the specified number of continuous response packets, it will identify a track as failure, i.e., the target tunnel is disconnected. • Src Address - Specifies the source IP address that sends Ping packets. • Dst Address - Specifies the IP address of the tracked object.
DNS1/2/3/4	Specifies the IP address of the DNS server allocated to the client by the PnPVPN server. You can define one primary DNS server and three backup DNS servers.
WINS1/2	Specifies the IP address of WINS server allocated to the client by the PnPVPN server. You can define one primary WINS server and a backup WINS server.
Tunnel Route	This item can be modified only after this IKE VPN is created. Click **Choose** to add one or more tunnel routes in the appearing Tunnel Route Configuration dialog box. You can

Advanced	
	add up to 128 tunnel routes.
Description	Type the description for the tunnel.
Smart Link	Select the smart link profile from the Smart Link drop-down list. For more information, see Configuring the Smart Link. Smart link and VPN Track cannot be configured simultaneously. **Note:** Only when the type of the peer IP is static support Smart Link.

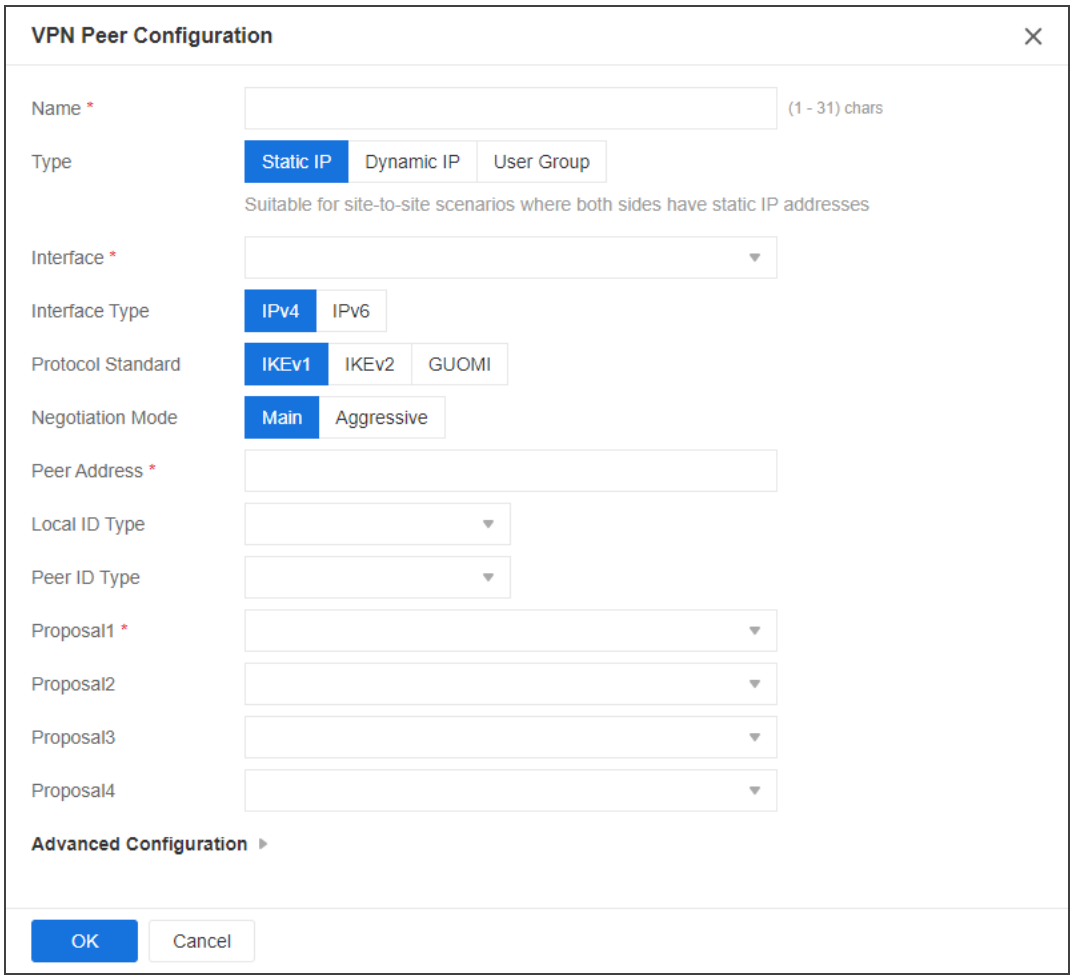
4. Click **OK** to save the settings.

Configuring a VPN Peer

To configure a VPN peer, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN tab, click **New**.

3. In the IPSec VPN Configuration page, select Peer Name drop-down list and click ⊕.



In the VPN Peer Configuration dialog box, configure the corresponding options.

Basic Configuration	
Name	Specifies the name of the ISAKMP gateway.
Type	Specifies the type of the peer IP. If the peer IP is static, type the IP address into the **Peer IP** box; if the peer IP type is user group, select the AAA server you need from the **AAA Server** drop-down list.
Interface	Specifies interface bound to the ISAKMP gateway.
Interface Type	Select the interface type, including IPv4 or IPv6. Only

Basic Configuration	
	the IPv6 firmware supports to configure IPv6 type interface.
Protocol Standard	Specifies the protocol standard, including IKEv1, IKEv2 and GUOMI . The default protocol standard is IKEv1. If you select GUOMI, specify the version: • v1.0: the version is 1.0. • v1.1: the version is 1.1. • Default: the initiator can negotiate with the peer when the initiator version is v1.0 or v1.1. Note: If you specify the version as 1.0 or 1.1, the version of the two peers which negotiate with each other should be the same, or system will fail to negotiate.
Negotiation Mode	Specifies the mode of IKE negotiation. There are two IKE negotiation modes: **Main** and **Aggressive**. The main mode is the default mode. The aggressive mode cannot protect identity. You have no choice but use the aggressive mode in the situation where the IP address of the center device is static and the IP address of client device is dynamic. Only IKEv1 and GUOMI support this option.
Local ID	Specifies the local ID. System supports five types of ID: FQDN, U-FQDN, Asn1dn (only for license), KEY-ID and IP. Select the ID type you want, and then type the content for this ID into the **Local ID** box or the **Local IP** box.
Peer ID	Specifies the peer ID. System supports five types of ID: FQDN, U-FQDN, Asn1dn (only for license), KEY-ID and IP. Select the ID type you want, and then type the

Basic Configuration	
	content for this ID into the **Peer ID** box or the **Peer IP** box.
Proposal1/2/3/4	Specifies a P1 proposal for ISAKMP gateway. Select the suitable P1 proposal from the **Proposal1** drop-down list. You can define up to four P1 proposals for an ISAKMP gateway. To create a P1 proposal, click ⊕. For detailed information, refer to Configuring a Phase 1 Proposal.
Pre-shared Key	If you choose to use pre-shared key to authenticate, type the key into the box.
Self-signed Trust Domain	If you choose to use RSA signature, ECDSA Signature or DSA signature, select a trust domain.
Peer Trust Domain	Configure the trust domain of peer certification. The peer certification is used for data encryption and authentication in the negotiation. The initiator should import the peer certification first. Only GUOMI v1.0 supports this option.
Encryption Trust Domain	Configure the trust domain of encryption certification. The encryption certification is used for data encryption in the negotiation. Only GUOMI v1.1 supports this option.

4. If necessary, click the **Advanced Configuration** tab to configure some advanced options.

In the Advanced Configuration tab, configure the corresponding options.

Advanced Configuration	
Connection Type	Specifies the connection type for ISAKMP gateway. • Bidirectional - Specifies that the ISAKMP gateway serves as both the initiator and responder. This is the default value.

Advanced Configuration	
	• Initiator - Specifies that the ISAKMP gateway serves as the only initiator. • Responder - Specifies that the ISAKMP gateway serves as the only responder.
NAT Traversal	This option must be enabled when there is a NAT device in the IPSec or IKE tunnel and the device implements NAT. By default, this function is disabled. Only IKEv1 and GUOMI support this option.
Any Peer ID	Makes the ISAKMP gateway accept any peer ID and not check the peer IDs. Only IKEv1 and GUOMI support this option.
Generate Route	Select the **Enable** check box to enable the auto routing function. By default, this function is disabled. This function allows the device to automatically add routing entries which are from the center device to the branch, avoiding the problems caused by manual configured routing.
DPD	Select the **Enable** check box to enable the DPD (Delegated Path Discovery) function. By default, this function is disabled. After the DPD function is enabled, the system will periodically send DPD requests to the peer in a specified time to detect whether the ISAKMP gateway exists. • DPD mode - Specify the DPD mode. • **periodic** - In this mode, the system continuously sends DPD requests to the peer at a specified interval. If no response packet is received from the peer within a DPD detection period, the sys-

Advanced Configuration	
	tem determines that the peer does not exist. DPD detection period=DPD Interval * DPD Retries. • **on-demand** - In this mode, the device does not send DPD requests if it receives no IPSec traffic. If the device receives IPSec traffic and needs to forward it, the system queries when the last receipt of the peer IPSec traffic happens. If the interval is shorter than the DPD detection period, it indicates that the peer ISAKMP gateway exists. In this case, the device does not send DPD detection requests. If the interval exceeds the DPD detection period, it indicates that the device needs to send DPD requests to detect the existence of the peer ISAKMP gateway. If the device does not receive the response packet during the DPD detection period, the system ages SA information in phase 1 and phase 2 and initiates a new IPSec negotiation. • DPD Interval - The interval of sending DPD request to the peer. The value range is 1 to 10 seconds. The default value is 10 seconds. • DPS Retries - The times of sending DPD request to the peer. The device will keep sending discovery requests

Advanced Configuration	
	to the peer until it reaches the specified times of DPD reties. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 10 times. The default value is 3.
Description	Type the description for the ISAKMP gateway.
XAUTH Server	Select **Enable** to enable the XAUTH server in the device. Then select an address pool from the drop-down list. After enabling the XAUTH server, the device can verify the users that try to access the IPSec VPN network by integrating the configured AAA server. Only IKEv1 and GUOMI support this option. You can select a configured IPSec-XAUTH address pool from the drop-down list. It is optional. When a client successfully connects to the XAUTH server, the server will take an IP address from the address pool and other parameters (like DNS server address or WIN server address) and assign them to the client. For more information about the IPSec-XAUTH address pool, see "VPN > IPsec Protocol > Configuring an IPsec VPN > XAUTH".

5. Click **OK** to save the settings.

Editing a VPN Peer

To edit a VPN peer, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN tab, click **New**.
3. In the IPSec VPN Configuration page, select Peer Name drop-down list and click .

Deleting a VPN Peer

To delete a VPN peer, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN tab, click **New**.
3. In the IPSec VPN Configuration page, select Peer Name drop-down list and click .

Copying a VPN Peer

You can quickly create a VPN peer by copying an existing one.

To copy a VPN peer, take the following steps:

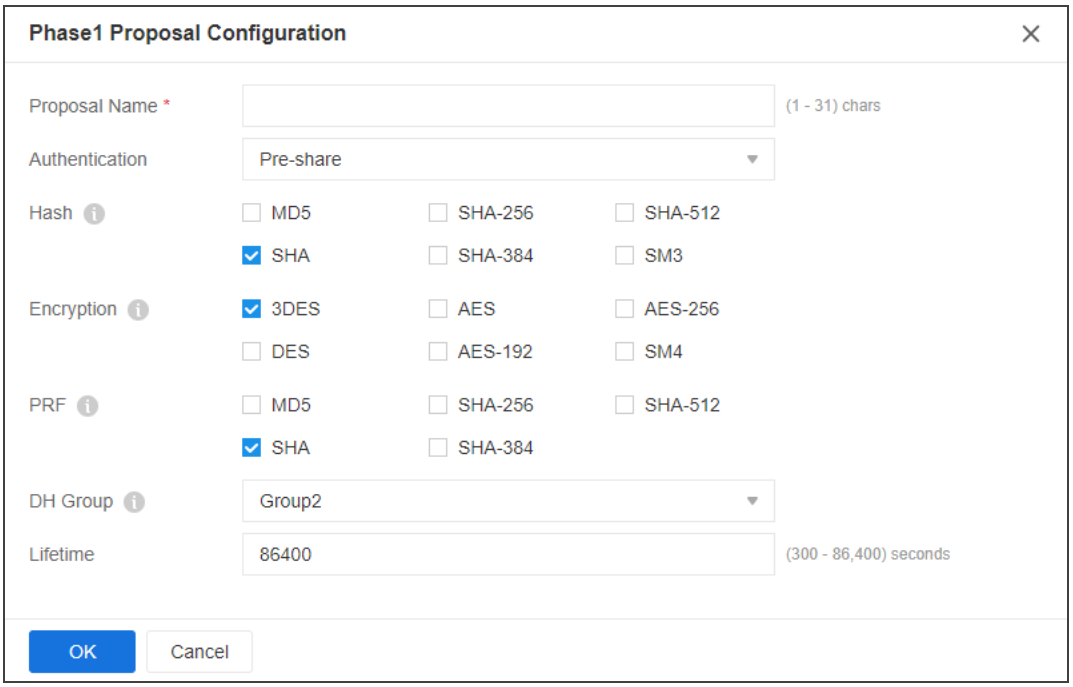
1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN tab, click **New**.
3. In the IPSec VPN Configuration page, select Peer Name drop-down list. Select the Peer that you want to copy and click . In the VPN Peer Configuration page, configure the parameters as required. The name of the peer cannot be the same as an existing one.
4. Click **OK**.

Configuring a Phase 1 Proposal

The P1 proposal is used to negotiate the IKE SA. To configure a P1 proposal, take the following steps:

1. In the IPSec VPN Configuration page, select Peer Name drop-down list and click .

2. In the VPN Peer Configuration page, select Proposal 1drop-down list and click ⊕.



In the Phase1 Proposal Configuration page, configure the corresponding options.

Option	Description
Proposal Name	Specifies the name of the Phase1 proposal.
Authentication	Specifies the IKE identity authentication method. IKE identity authentication is used to verify the identities of both communication parties. There are three methods for authenticating identity: pre-shared key, RSA signature, ECDSA Signature, DSA signature and GM-DE. The default value is pre-shared key. For pre-shared key method, the key is used to generate a secret key and the keys of both parties must be the same so that it can generate the same secret keys.
Hash	Specifies the authentication algorithm for Phase1. Select the algorithm you want to use. • MD5 – Uses MD5 as the authentication algorithm.

Option	Description
	Its hash value is 128-bit. • SHA – Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 – Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 – Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 – Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit. • SM3 – Use the state password SM3 as the authentication algorithm. Its hash value is 256-bit. It is used for the digital signature and authentication, the generation and authentication of message authentication code, and the generation of random digit, which can meet the security requirement of multiple password applications. Only IKEv1 supports this option.
Encryption	Specifies the encryption algorithm for Phase1. • 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES – Uses DES as the encryption algorithm. The

Option	Description
	key length is 64-bit. • AES – Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 – Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 – Uses 256-bit AES as the encryption algorithm. The key length is 256-bit. • SM4 – Uses the state password SM4 as the encryption algorithm. The key length is 128-bit. Only IKEv1 supports this option.
PRF	Specifies the PRF algorithms for Phase1. Only IKEv2 supports this option. • MD5 – Uses the MD5 algorithm. The digest length is 128 bits. • SHA – Uses the SHA-1 algorithm. The digest length is 160 bits. This is the default hash algorithm. • SHA-256 – Uses the SHA-256 algorithm. The digest length is 256 bits. • SHA-384 – Uses the SHA-384 algorithm. The digest length is 384 bits. • SHA-512 – Uses the SHA-512 algorithm. The digest length is 512 bits.

Option	Description
DH Group	Specifies the DH group for Phase1 proposal. • Group1 – Uses Group1 as the DH group. The key length is 768-bit (MODP Group). • Group2 – Uses Group2 as the DH group. The key length is 1024-bit (MODP Group). Group2 is the default value. • Group5 – Uses Group5 as the DH group. The key length is 1536-bit (MODP Group). • Group14 – Uses Group14 as the DH group. The key length is 2048-bit (MODP Group). • Group15 – Uses Group5 as the DH group. The key length is 3072-bit (MODP Group). • Group16 – Uses Group16 as the DH group. The key length is 4096-bit (MODP Group). • Group18 – Uses Group18 as the DH group. The key length is 8192-bit (MODP Group). • Group19 - Uses Group 19 as the DH group. The key length is 256 bits (ECP Group). • Group20 - Uses Group 20 as the DH group. The key length is 384 bits (ECP Group). • Group21 - Uses Group 21 as the DH group. The key

Option	Description
	length is 521 bits (ECP Group). • Group24 - Uses Group 24 as the DH group. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).
Lifetime	Specifies the lifetime of SA Phase1. The value range is 300 to 86400 seconds. The default value is 86400. Type the life-time value into the Lifetime box. When the SA lifetime runs out, the device will send a SA P1 deleting message to its peer, notifying that the P1 SA has expired and it requires a new SA negotiation.

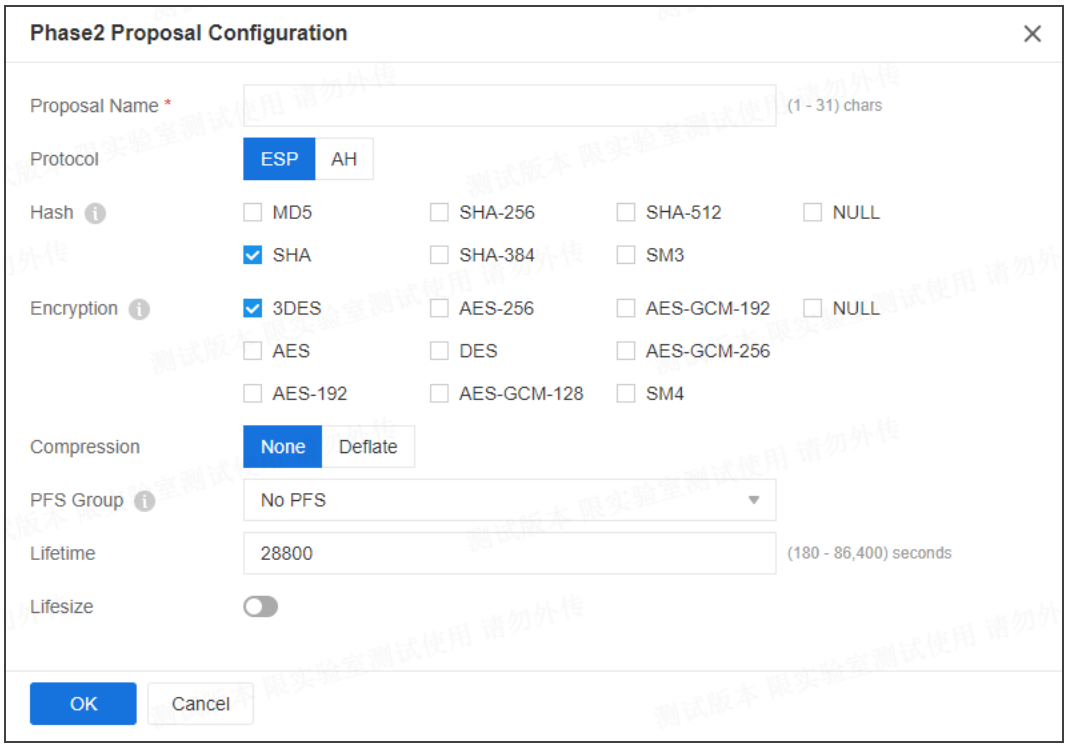
3. Click **OK** to save the settings.

Configuring a Phase 2 Proposal

The P2 proposal is used to negotiate the IPSec SA. To configure a P2 proposal, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN tab, click **New**.

3. In the IPSec VPN Configuration page, select P2 Proposal drop-down list and click ⊕.



In the Phase2 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Proposal Name	Specifies the name of the Phase2 proposal.
Protocol	Specifies the protocol type for Phase2. The options are ESP and AH. The default value is ESP.
Hash	Specifies the authentication algorithm for Phase2. Select the algorithm you want to use. • MD5 – Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA – Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm.

Option	Description
	• SHA-256 – Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 – Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 – Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit. • SM3 – Uses the state password SM3 as the authentication algorithm. Its hash value is 256-bit. It is used for the digital signature and authentication, the generation and authentication of message authentication code, and the generation of random digit, which can meet the security requirement of multiple password applications. • Null – No authentication.
Encryption	Specifies the encryption algorithm for Phase2. • 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES – Uses DES as the encryption algorithm. The key length is 64-bit. • AES – Uses AES as the encryption algorithm. The key length is 128-bit.

Option	Description
	• AES-192 – Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 – Uses 256-bit AES as the encryption algorithm. The key length is 256-bit. • AES-GCM-128 – Uses 128-bit AES-GCM as the encryption algorithm. The key length is 128-bit. • AES-GCM-192 – Uses 192-bit AES-GCM as the encryption algorithm. The key length is 192-bit. • AES-GCM-256 – Uses 256-bit AES-GCM as the encryption algorithm. The key length is 256-bit. • SM4 – Uses the state password SM4 as the encryption algorithm. The key length is 128-bit. • Null – No authentication.
Compression	Specifies the compression algorithm for Phase2. By default, no compression algorithm is used.
PFS Group	Specifies the PFS function for Phase2. PFS is used to protect DH algorithm. • No PFS - Disables PFS. This is the default value. • Group1 – Uses Group1 as the DH group. The key length is 768-bit (MODP Group). • Group2 – Uses Group2 as the DH group. The key length is 1024-bit (MODP Group).

Option	Description
	• Group5 – Uses Group5 as the DH group. The key length is 1536-bit (MODP Group). • Group14 – Uses Group14 as the DH group. The key length is 2048-bit (MODP Group). • Group15 – Uses Group15 as the DH group. The key length is 3072-bit. • Group16 – Uses Group16 as the DH group. The key length is 4096-bit (MODP Group). • Group18 – Uses Group18 as the DH group. The key length is 8192-bit (MODP Group). • Group19 - Uses Group 19 as the DH group. The key length is 256 bits (ECP Group). • Group20 - Uses Group 20 as the DH group. The key length is 384 bits (ECP Group). • Group21 - Uses Group 21 as the DH group. The key length is 521 bits (ECP Group). • Group24 - Uses Group 24 as the DH group. The key length is 2048 bits (MODP Group with 256-bit Prime Order Subgroup).
Lifetime	You can evaluate the lifetime by two standards which are the time length and the traffic volume. Type the lifetime length of P2 proposal into the box. The value range is 180 to 86400 seconds. The default value is 28800.

Option	Description
Lifesize	Select **Enable** to enable the P2 proposal traffic-based lifetime. By default, this function is disabled. After selecting Enable, specifies the traffic volume of lifetime. The value range is 1800 to 4194303 KBs. The default value is 1800. Type the traffic volume value into the box.

4. Click **OK** to save the settings.

Configuring the Smart Link

When there are multiple communication links between branches and the headquarter data center, you can configure Smart Link on branch firewalls to realize dynamic switch between IPSec links. Each link has a unique ID. With the Smart Link function, the system selects the link by order to negotiate the IPSec tunnel. To view or adjust the link order, go to **Network** > **VPN** > **IPSec VPN**. In the initial state, the system selects the top link to negotiate an IPSec tunnel. When the IPSec tunnel is established, the system sends detection packets to detect link quality. If the packet loss rate or latency exceeds the specified threshold, the system would switch the current link to the next one to establish a new IPSec tunnel.

Notes: The smart link function can only be configured when the type of the VPN peer is static IP.

To configure the smart link, take the following steps:

1. Select **Network** > **VPN** > **IPSec VPN**.
2. Select the **IPSec VPN** tab
3. Click **New** to go to the **IPSec VPN Configuration** page.
4. Click the **Smart Link** drop-down list and then click + to expand the **Smart Link Configuration** section.

Configure the following options.

Smart Link Configuration	
Name	Specifies the name of the smart link profile. You can enter up to 31 characters.
Link for Negotiation	Click **New** to configure the link's local interface and peer IP address. Click **Batch Add** to add links in batches. One smart link profile supports up to three local interfaces and ten peer IP addresses (30 links in total). You can configure both IPv4 and IPv6 addresses for the link to negotiate an IPSec tunnel. But one smart link profile only supports one IP type (either IPv4 or IPv6). New links are arranged from top to bottom based on the configuration sequence.
Link Detection	Click the button to enable Link Detection. This function is enabled by default.
Source Address	Specifies the source IP address of the detection packets.If this field is not specified, the IP address of the IPSec tunnel's local interface is used as the source IP address of the detection packets. By default, this field is blank.
Destination Address	Specifies the destination IP address of the detection packets.If this field is not specified, the IP address of the IPSec tunnel's peer interface is used as the destination IP address of the detection packets. By default, this field is blank.
Detection Interval	Specifies the interval to send detection packets. The value range is from 1 to 5 seconds. The default value is 3 seconds.
Total Number of Detection Pack-	Specifies the total number of detection packets sent in a detection period. The value range is from 1 to 30. The

Smart Link Configuration	
ets	default value is 10.
Link Quality Parameters	Select the link quality parameter and configure its threshold. After a detection period, the system calculates the link's latency and packet loss rate, and compares the value to the threshold. The system will switch the current link to the next one if either parameter exceeds its threshold. The value range of latency is from 100 to 3000 milliseconds. The default value is 500. The value range of packet loss rate is from 1 to 100 percent. The default value is 30.
Cycle Switching Times	Specifies the threshold for the cycle switching times. The value range is from 0 to 5. The default value is 5. The value 0 indicates that there is no limit to the cycle switching times. When all links are switched in turn, it is called a switch cycle. If the cycle switching times exceed the threshold, the system will no longer detect and switch links and will switch the current link to the one with the best quality.
Quiet Time of Switch	Specifies the silence period after the cycle switching times exceed the threshold. If the cycle switching times exceed the threshold, the system will no longer detect and switch links. The default silence period is 600 seconds. When the silence period expires, the system starts to detect the quality of the active link again. The value range is from 600 to 1800 seconds.

To manage IPSec links, take the following steps:

1. Select **Network** > **VPN** > **IPSec VPN**.
2. Select the **IPSec VPN** tab
3. Expand the selected IPSec VPN to view all the configured IPSec links, including the one currently in Active state. You can also view latency and packet loss rate of each link.
4. Click the up and down arrow in the Operation column to adjust the sequence of the links. Click the **Active** button to activate the specified link for immediate IPSec tunnel negotiation.

Editing an IPSec VPN

To edit an IPSec VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. Select the IPSec VPN entries to be edited in the IPSec VPN list. Click **Edit** and modify the configurations in the IPSec VPN Configuration page.

Deleting an IPSec VPN

To delete an IPSec VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN tab, select the IPSec VPN you want to delete.
3. Click **Delete**.

If an IPSec VPN is associated with a tunnel interface, security policy, GRE VPN or L2TP VPN, to delete it, you need to unreference/delete the associated items first. You can navigate to related modules to unreference/delete the associated items or unreference/delete them directly in the IPSec VPN tab:

1. Select the IPSec VPN to be deleted and click **Delete**.
2. A prompt is displayed, asking whether to unreference/delete all the associated items of the IPSec VPN. Click **Delete** to unreference/delete all associated items and the selected IPSec VPN; Click **Cancel** to return to the IPSec VPN tab; Click **View Details** to switch to the Referenced by page.
3. In the Referenced by page, click the security policy ID, tunnel interface name, GRE VPN name or L2TP VPN name in the "Object" column to view the configuration information of each associated item. Click **Unreference** or **Delete** in the "Operation" column to unreference/delete each associated item respectively.

Tips: When any of the selected IPSec VPN entries has an associated item, the IPSec VPN entries cannot be deleted in batches. When you delete an IPSec VPN entry with associated items, the system supports deletion of 5000 associated items at most. If the number of associated items exceeds 5000, you need to perform the IPSec VPN deletion again.



Notes:

- When any of the selected IPSec VPN entries has an associated item, the IPSec VPN entries cannot be deleted in batches.
- When you delete an IPSec VPN entry with associated items, the system supports deletion of 5000 associated items at most. If the number of associated items exceeds 5000, you need to perform the IPSec VPN deletion again.

Enabling or Disabling an IPSec VPN

To enable or disable an IPSec VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN Configuration tab, select one or more IPSec VPN from the IPSec VPN list.
3. Click **Enable** or **Disable**. The enabled status is displayed as  .

Copying an IPSec VPN

You can quickly create an IPSec VPN by copying an existing one.

To copy an IPSec VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN Configuration tab, select the IPSec VPN that you want to copy and click **Copy**. In the IPSec VPN Configuration page, configure the parameters as required. The name of the tunnel cannot be the same as an existing one.
3. Click **OK**.

Viewing IPSec VPN Entry

To view an IPSec VPN entry of specified filter condition, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN tab, enter the name of the IPSec VPN entry or the peer name in the text boxes at the top of the toolbar to view the IPSec VPN entry under the specified conditions.
3. Click the value in the "Referenced by" column to view the details of the configuration items associated with an IPSec VPN entry.

Configuring a Manual Key VPN

Manually configuring SA is complicated as all the information will be configured by yourself and some advanced features of IPSec are not supported (e.g. timed refreshing), but the advantage is that manually configured SA can independently fulfill IPSec features without relying on IKE. This method applies to a situation with a small number of devices or an environment of static IP addresses.

To create a manual key VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the Manual Key VPN Configuration section, click **New**.

Basic Configuration	
Tunnel Name	Specifies the name of manually created key VPN.
Encapsulation Mode	Specifies the encapsulation mode, including Tunnel and Transport. The tunnel mode is the default mode.
Peer IP	Specifies the IP address of the peer.
Local SPI	Type the local SPI value. SPI is a 32-bit value transmitted in AH and ESP header, which uniquely identifies a security association. SPI is used to seek corresponding VPN tunnel for decryption.
Remote SPI	Type the remote SPI value. **Note**: When configuring an SA, you should configure the parameters of both the inbound and outbound direction. Furthermore, SA parameters of the two ends of the tunnel should be totally matched. The local inbound SPI should be the same with the outbound SPI of the other end; the local outbound SPI should be the same with the inbound SPI of the other end.

Basic Configuration	
Interface	Specifies the egress interface for the manual key VPN. Select the interface you want from the **Interface** drop-down list.
Interface Type	Select the interface type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type interface.
Encryption	
Protocol	Specifies the protocol type. The options are ESP and AH. The default value is ESP.
Encryption	Specifies the encryption algorithm. • None – No authentication. • 3DES – Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES – Uses DES as the encryption algorithm. The key length is 64-bit. • AES – Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 – Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 – Uses 256-bit AES as the encryption algorithm. The key length is 256-bit.
Inbound Encryption Key	Type the encryption key of the inbound direction. You should configure the keys of both ends of the tunnel. The local

Basic Configuration	
	inbound encryption key should be the same with the peer's outbound encryption key, and the local outbound encryption key should be the same with the peer's inbound encryption key.
Outbound Encryption Key	Type the encryption key of the outbound direction.
Hash	Specifies the authentication algorithm. Select the algorithm you want to use. • None – No authentication. • MD5 – Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA-1 – Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 – Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 – Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 – Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit.
Inbound Hash Key	Type the hash key of the inbound direction. You should configure the keys of both ends of the tunnel. The local inbound hash key should be the same with the peer's outbound hash key, and the local outbound hash key should be the same with the

Basic Configuration	
	peer's inbound hash key.
Outbound Hash Key	Type the hash key of the outbound direction.
Compression	Select a compression algorithm. By default, no compression algorithm is used.
Description	
Description	Type the description for the manual key VPN.

3. Click **OK** to save the settings.

Deleting a Manual Key VPN

To delete a manual key VPN, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the Manual Key VPN Configuration tab, select the manual key VPN you want to delete.
3. Click **Delete**.

If a manual key VPN is associated with a tunnel interface, security policy, GRE VPN or L2TP VPN, to delete it, you need to unreference/delete the associated items first. You can navigate to related modules to unreference/delete the associated items or unreference/delete them directly in the Manual Key VPN Configuration tab:

1. Select the manual key VPN entry to be deleted and click **Delete**.
2. A prompt is displayed, asking whether to unreference/delete all the associated items of the manual key VPN entry. Click **Delete** to unreference/delete all the associated items and the selected manual key VPN; Click **Cancel** to return to the Manual Key VPN Configuration tab; Click **View Details** to switch to the Referenced by page.

3. In the Referenced by page, click the security policy ID, tunnel interface name, GRE VPN name or L2TP VPN name in the "Object" column to view the configuration information of each associated item. Click **Unreference** or **Delete** in the "Operation" column to unreference/delete each associated item respectively.



Notes:

- When any of the selected manual key VPN entries has an associated item, the manual key VPN entries cannot be deleted in batches.
- When you delete a manual key VPN entry with associated items, the system supports deletion of 5000 associated items at most. If the number of associated items exceeds 5000, you need to perform the manual key VPN deletion again.

Viewing Manual Key VPN Entry

To view a manual key VPN of specified filter condition, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the Manual Key VPN Configuration section, enter the name of the manual key VPN entry in the text box at the top of the toolbar to view the manual key VPN entry under the specified conditions.
3. Click the value in the "Referenced by" column to view the details of the configuration items associated with a manual key VPN entry.

Viewing IPSec VPN Monitoring Information

By using the ISAKMP SA table, IPSec SA table, and Dial-up User table, IPSec VPN monitoring function can show the SA negotiation results of IPSec VPN Phase1 and Phase2 as well as information of dial-up users.

To view the VPN monitoring information, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. In the IPSec VPN page, click **IPSec VPN Monitor** . You can view IPSec VPN monitoring information in ISAKMP SA, IPSec SA and Dial-up User tabs.
    - In the ISAKMP SA page, you can specify the peer name in the "Peer" drop-down menu and filter the monitoring information by the peer name;
    - In the IPSec SA page, you can specify the VPN name in the "VPN Name" drop-down menu and filter the monitoring information by the VPN name;
    - In the Dial-up User page, you can specify the peer name in the "Peer Name" drop-down menu and filter monitoring information by the peer name. You can also click 

and filter monitoring information by IKE ID, dialed-in user, and private IP.

Options in these tabs are described as follows:

ISAKMP SA

Option	Description
Peer	Displays the peer name.
Cookie	Displays the negotiation cookies which are used to match SA Phase 1.
Protocol Stand-ard	Displays the protocol standard used for negotiation.
Status	Displays the status of SA Phase1.
Peer Address	Displays the IP address of the peer.
Port	The port number used by the SA Phase1. 500 indicates that no NAT has been found during the SA Phase 1; 4500 indicates that NAT has been detected.
Algorithm	Displays the algorithm of the SA Phase1, including authentication

Option	Description
	method, encryption algorithm and verification algorithm.
Lifetime	Displays the lifetime of SA Phase1. The unit is second.

IPSec SA

Option	Description
ID	Displays the tunnel ID number which is auto assigned by the system.
VPN Name	Displays the name of VPN.
Protocol Standard	Displays the protocol standard used for negotiation.
Peer Name	Displays the name of the peer.
Direction	Displays the direction of VPN.
Peer Address	Displays the IP address of the peer.
Port	The port number used by the SA Phase2.
Algorithm	The algorithm used by the tunnel, including protocol type, encryption algorithm, verification algorithm and depression algorithm.
SPI	Displays the local SPI and the peer SPI. The direction of inbound is local SPI, while outbound is peer SPI.
CPI	Displays the compression parameter index (CPI) used by SA Phase2.
Lifetime (s)	Displays the lifetime of SA Phase2 in seconds, i.e. SA Phase2 will restart negotiations after X seconds.
Lifetime (KB)	Displays the lifetime of SA Phase2 in KB, i.e. SA Phase2 will restart negotiations after X kilobytes of data flow.
Status	Displays the status of SA Phase2.

Option	Description
Traffic	Displays the cumulative value of the inbound and outbound traffic of the tunnel.
Protect Network	Displays the protect network of the tunnel.
Duration (second)	Displays the duration starting from the latest successful SA negotiation of Phrase 2 to the current time. The duration is measured by second.
Sending/Receiving Rate (KB/s)	Displays the real-time sending/ receiving rate when the tunnel sends/receives packets. Outbound packets are associated with the sending rate while inbound packets are associated with the receiving rate. The unit is KB/s.
Last Setup Time	Displays the last setup time of the latest SA negotiation of Phrase 2.
Last Teardown Time	Displays the time when the latest SA teardown of Phrase 2 occurs.
Teardown Reason	Displays the reasons for the latest SA teardown of Phrase 2: • a disconnection request is received from the peer • an idle connection timeout occurred • configuration changed • VPN is manually cleared • a DPD timeout occurred • VPN track failed • an SPI inconsistency error occurred • a lifetime timeout occurred

Option	Description
Teardowns Today	Displays the counts of SA teardown of Phrase 2 from 0:00 on the current day to the current time. The system starts counting the SA teardowns of Phrase 2 as early as 0:00 on the day and has to stop counting before 0:00 on the next day. After 0:00 on the next day, the previous counts are cleared to 0.

Dial-up User

Option	Description
IKE ID	Displays the IKE ID of the user selected.
Dialed-in User	Displays the name of the dialed-in user.
Public IP	Displays the public IP address of the dialed-in user.
Private IP	Displays the private IP address of the dialed-in user.
Encrypted Packets	Displays the number of encrypted packets transferred through the tunnel.
Encrypted Bytes	Displays the number of encrypted bytes transferred through the tunnel.
Decrypted Packets	Displays the number of decrypted packets transferred through the tunnel.
Decrypted Bytes	Displays the number of decrypted bytes transferred through the tunnel.

Configuring PnPVPN

IPSec VPN requires sophisticated operational skills and high maintenance cost. To relieve network administrators from the intricate work, system provides an easy-to-use VPN technology -

PnPVPN (Plug-and-Play VPN). PnPVPN consists of two parts: PnPVPN Server and PnPVPN Client.

- PnPVPN Server: Normally deployed in the headquarters and maintained by an IT engineer, the PnPVPN Server sends most of the configuration commands to the clients. The device usually works as a PnPVPN Server and one device can serve as multiple servers.
- PnPVPN Client: Normally deployed in the branch offices and controlled remotely by a headquarters engineer, the PnPVPN Client can obtain configuration commands (e.g. DNS, WINS, DHCP address pool, etc.) from the PnPVPN Server with simple configurations, such as client ID, password, and server IP settings.

The device can serve as both a PnPVPN Server and a PnPVPN Client. When working as a PnPVPN Server, the maximum number of VPN instance and the supported client number of each device may vary according to the platform series.

PnPVPN Workflow

The workflow for PnPVPN is as follows:

1. The client initiates a connection request and sends his/her own ID and password to the server.
2. The server verifies the ID and password when it receives the request. If the verification succeeds, the server will send the configuration information, including DHCP address pool, DHCP mask, DHCP gateway, WINS, DNS and tunnel routes, etc,. to the client.
3. The client distributes the received information to corresponding functional modules.
4. The client PC automatically gains an IP address, IP mask, gateway address and other network parameters and connects itself to the VPN.

PnPVPN Link Redundancy

The PnPVPN server supports dual VPN link dials for a PnPVPN client, and automatically generates the routing to the client. Also, it can configure the VPN monitor for the client. Two ISAKMP gateways and two tunnel interfaces need to be configured in the server. The two VPN tunnels need to refer different ISAKMP gateways and be bound to different tunnel interfaces.

The client supports to configure dual VPN dials and redundant routing. When the two VPN tunnels are negotiating with the server, the client generates routes with different priority according to the tunnel routing configuration at the server side. The high priority tunnel acts as the master link and the tunnel with low priority as the backup link, so as to realize redundant routing. The master VPN tunnel will be in the active state first. When master tunnel is interrupted, the client will use the backup tunnel to transfer the data. When the master tunnel restores to be normal, it will transfer the data again.

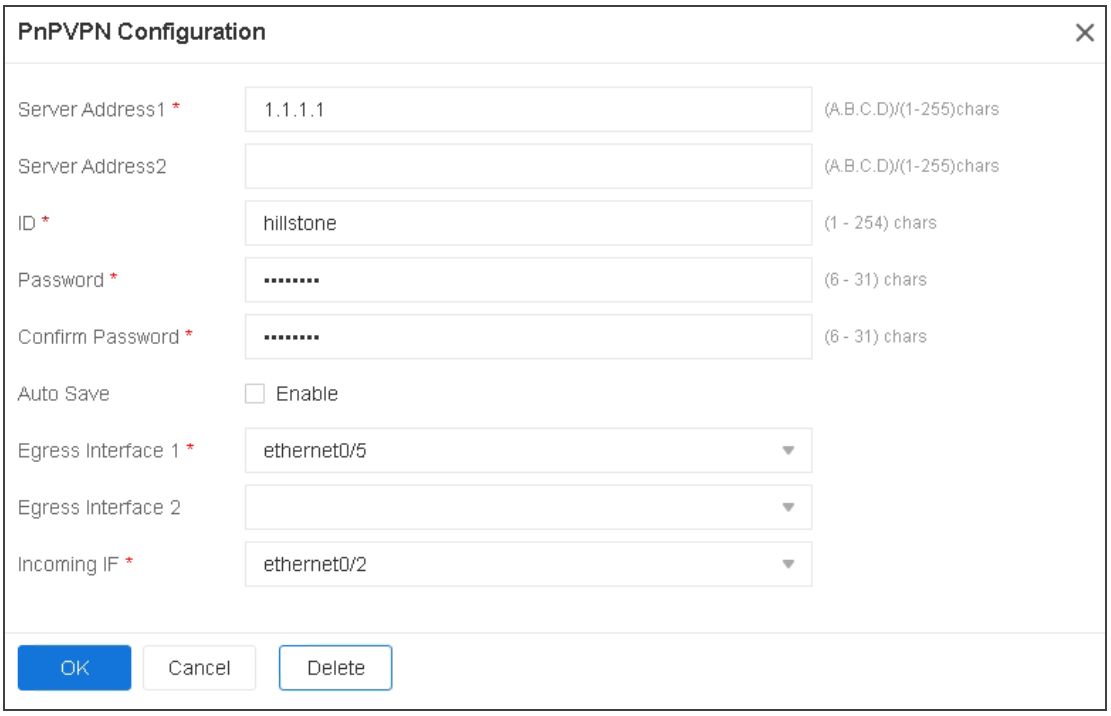
Configuring a PnPVPN Client

To configure a PnPVPN client, take the following steps:

1. Select **Network > VPN > IPSec VPN**.

2. At the top right corner of the IKE VPN Configuration section, click **Configuration**, selcet

PnPVPN Configuration from the drop-down list.



Option	Description
Server Address1	Type the IP address of PnPVPN Server into the box. PnPVPN client supports dual link dials to the server side. This option is required.
Server Address2	Type the IP address of PnPVPN Server into the box. The server address 1 and the server address 2 can be the same or different. It is optional.
ID	Specifies the IKE ID assigned to the client by the server.
Password	Specifies the password assigned to the client by the server.
Confirm Password	Enter the password again to confirm.
Auto Save	Select Enable to auto save the DHCP and WINS information

Option	Description
	released by the PnPVPN Server.
Egress Interface 1	Specifies the interface connecting to the Internet. This option is required.
Egress Interface 2	Specifies the interface connecting to the Internet. The IF1 and the IF2 can be the same or different. It is optional.
Incoming IF	Specifies the interface on the PnPVPN Client accessed by the Intranet PC or the application servers.

3. Click **OK** to save the settings.



Notes:

- Server Addresses1 and Egress IF1 both need to be configured. If you want to configure a backup link, you need to configure both the Server Address2 and Egress IF2.
- If the server addresses or the Egress IFs are different, two separate VPN links will be generated.
- The configuration of the two servers can be configured on one device, and can also be configured on two different devices. If you configure it on two devices, you need to configure AAA user on the two devices. The DHCP configuration for the AAA user should be the same, otherwise it might cause that the client and server negotiate successfully, but the traffic is blocked.

Configuring IPSec-XAUTH Address Pool

XAUTH server assigns the IP addresses in the address pool to users. After the client has established a connection to the XAUTH server successfully, the XAUTH server will choose an IP

address along with other related parameters (such as DNS server address, WINS server address, etc) from the address pool, and will assign them to the client.

XAUTH server provides fixed IP addresses by creating and implementing IP binding rules that consist of a static IP binding rule and an IP-role binding rule. The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, system will assign the binding IP to the client. The IP-role binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, system will assign an IP address within the IP range to the client.

When the XAUTH server is allocating IP addresses in the address pool, system will check the IP binding rule and determine how to assign IP addresses to the client based on the specific checking order below:

1. Check if the client is configured with any static IP binding rule. If so, assign the binding IP address to the client; otherwise, check the other configuration. Note if the binding IP address is in use, the user will be unable to log in.
2. Check if the client is configured with any IP-role binding rule. If so, assign an IP address within the binding IP range to the client; otherwise, the user will be unable to log in.

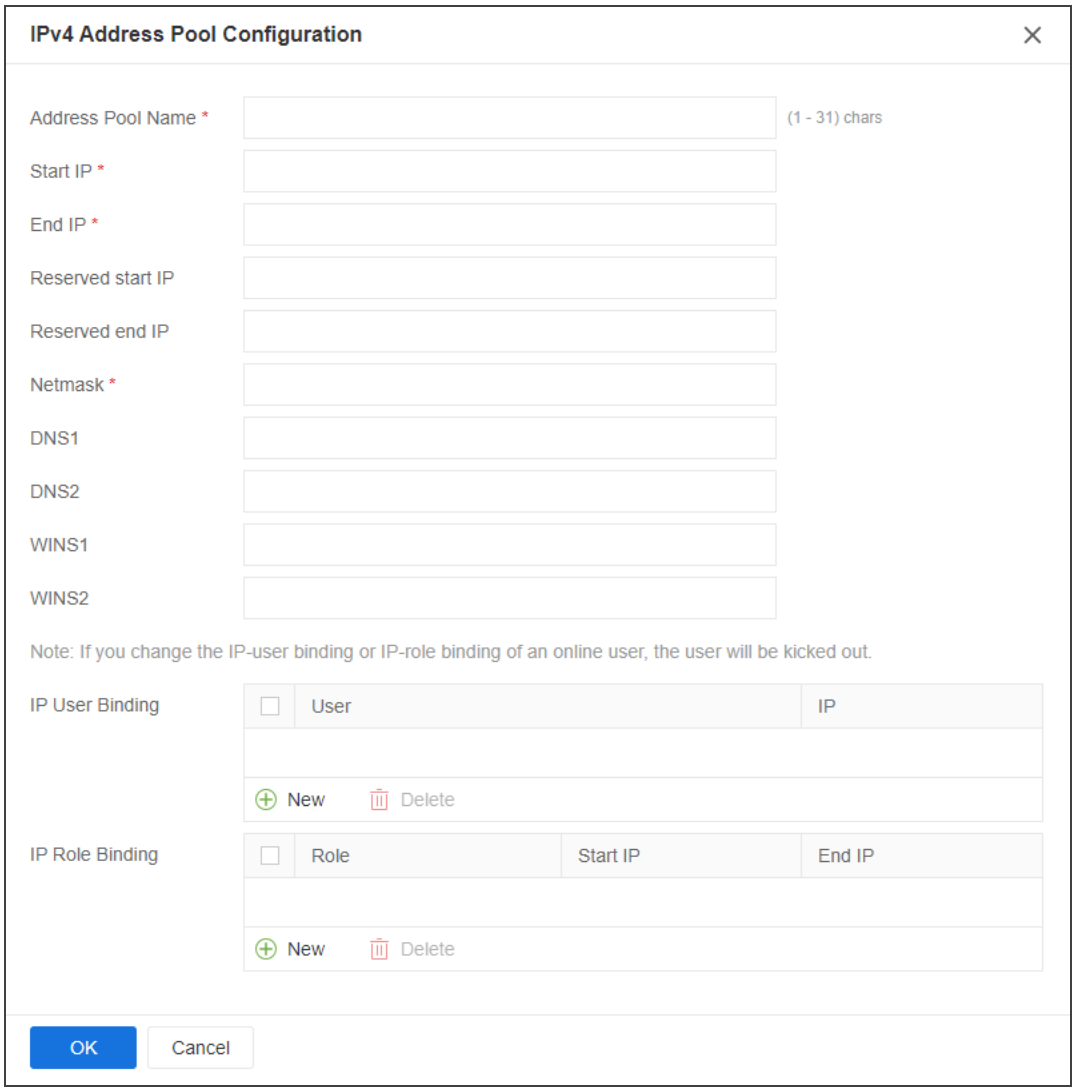


Notes: The IP addresses defined in the static IP binding rule and IP-role binding rule should not be overlapped.

To configure the IPSec-XAUTH address pool, take the following steps:

1. Select **Network > VPN > IPSec VPN**.
2. At the top-right corner, select **Configuration** > **IPSec-XAUTH Address Pool.**.
3. Select the **IPv4** or **IPv6** tab. The IPv6 tab is available only when the version is in IPv6.

4. Click **New**.



In the Basic Configuration tab, configure the corresponding options.

Option	Description
Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IPv4 or IPv6 address of the address pool.
End IP	Specifies the end IPv4 or IPv6 address of the address pool.
Reserved	Specifies the reserved start IPv4 or IPv6 address of the

Option	Description
Start IP	address pool.
Reserved End IP	Specifies the reserved end IPv4 or IPv6 address of the address pool.
Netmask	Specifies the netmask of the IPv4 address.
Prefix Length	Specifies the prefix length of the IPv6 address.
DNS1/2	Specifies the DNS server IP address for the address pool. It is optional. At most two DNS servers can be configured for one address pool.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to two WIN servers can be configured for one address pool. This option is supported only by IPv4.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the **User** box.
IP	Type the IP address into the **IP** box.
Add	Click **Add** to add the item that binds the specified user to the IP address.

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Select a role from the **Role**drop-down list.
Start IP	Type the start IP address into the **Start IP** box.
End IP	Type the end IP address into the **End IP** box.
Add	Click **Add** to add the item that binds the specified role to the IP address range.
Up/Down/Top/Bottom	Move the selected IP-role binding rule . For the

Option	Description
	user that is bound to multiple roles that are also configured with their corresponding IP-role binding rules, system will query the IP-role binding rules in order, and assign an IP address based on the first matched rule.

5. Click **OK** to save the settings.

SSL VPN

The device provides an SSL based remote access solution. Remote users can access the intranet resource safely through the provided SSL VPN.

SSL VPN consists of two parts: SSL VPN server and SSL VPN client. The device configured as the SSL VPN server provides the following functions:

- Accept client connections.
- Allocate IP addresses, DNS server addresses, and WIN server addresses to SSL VPN clients.
- Authenticate and authorize clients.
- Perform host checking to client.
- Decrypting and forwarding encrypted packet from the client.

By default, the concurrent online client number may vary on different platform series. You can expand the supported number by purchasing the corresponding license.

After successfully connecting to the SSL VPN server, the SSL VPN client secures your communication with the server. The following SSL VPN clients are available:

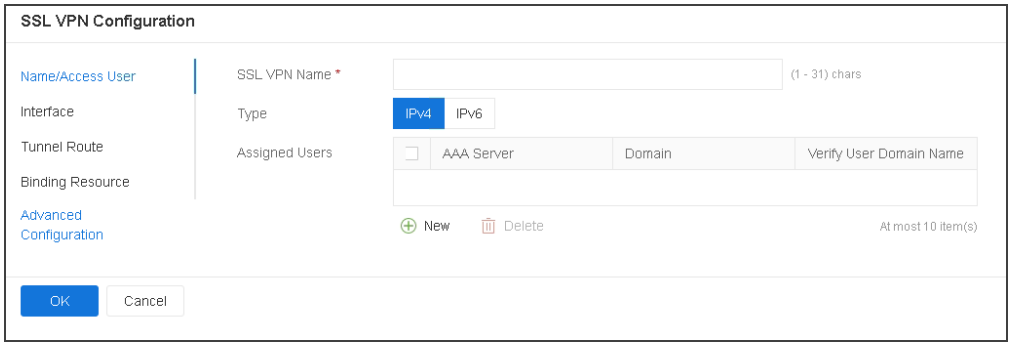
- "Hillstone Secure Connect Client for Windows" on Page 644
- "Hillstone Secure Connect Client for Android" on Page 662
- "Hillstone Secure Connect Client for iOS" on Page 669

- "Hillstone Secure Connect Client for macOS" on Page 675
- "Hillstone Secure Connect Client for Linux" on Page 686
- "Hillstone Secure Connect Client for ChineseOS" on Page 697

Configuring an SSL VPN

To configure an SSL VPN, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. In the SSL VPN page, click **New**.



In the Name/Access User tab, configure the corresponding options.

Option	Description
SSL VPN Name	Type the name of the SSL VPN instance.The length is 1 to 64 characters.
Type	Select IPv4 or IPv6 to specify the service type of the SSL VPN instance. This option can only be configured when the version is IPv6.
Assigned Users (at most 10 items)	
AAA Server	Select an AAA server from the **AAA Server** drop-down list. You can click **View AAA Server** to view the detailed information of this AAA server. If you select an OAuth2 server, the client supports OAuth2 authentication.

Option	Description
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server.The length is 1 to 31 characters.
Verify User Domain Name	After enabling this function, system will verify the username and its domain name. **Note**: The OAuth2 server does not support user domain name verification.
Add	Click **Add** to add the assigned users. You can repeat to add more items.

In the Interface tab, configure the corresponding options.

Access Interface	
Egress Interface	Select the interface from the drop-down list as the SSL VPN server interface. This interface is used to listen to the request from the SSL VPN client. At most 8 interfaces can be selected.
Service Port	Specifies the SSL VPN service port number.The value range is 1 to 65535.
Tunnel Interface	
Tunnel Interface	Specifies the tunnel interface used to bind to the SSL VPN tunnel. Tunnel interface transmits traffic to/from SSL VPN tunnel. • Select a tunnel interface from the drop-down list, and then click **Edit** to edit the selected tunnel interface. • Click **New** in the drop-down list to create a new interface.

Access Interface	
Address Pool	
Address Pool	Specifies the SSL VPN address pool. • Select an address pool from the drop-down list, and then click **Edit** to edit the selected address pool. • Click **New** in the drop-down list to create a new address pool. When configuring IPv6 SSL VPN, this option specifies the IPv6 SSL VPN address pool.

In the Tunnel Route tab, configure the following options.

Tunnel Route	
Specifies the destination network segment that you want to access through SSL VPN tunnel. The specified destination network segment will be distributed to the VPN client, then the client uses it to generate the route to the specified destination. A maximum of 128 tunnel routes based on network segments can be added for an SSL VPN instance.	
New	Click **New** to add this route. You can repeat to add more items.
IP	Type the destination IP address.
Mask	Type the netmask of the destination IP address.
Metric	Type the metric value.
Type	Sets the user type to **User Group** or **Role**.
User Group/Role	When the type is set to **User Group**, select the AAA server to which the user group belongs and the user group name from the drop-down list. Only users in this user group can access the specified network segment

Tunnel Route	
	in the tunnel route. You can also click ⊕ and create a user group in the **User Group Configuration** panel. For more information, see Creating a User Group. When the type is set to **Role**, select the role name from the drop-down list. Only users corresponding to this role can access the specified network segment in the tunnel route. You can also click ⊕ and create a role in the **Role Configuration** panel. For more information, see Creating a Role.
Delete	Click **Delete** to delete the selected route.
Add Default Route	Click **Add Default Route** to add a default route with both the IP address and netmask being all 0.
Enable Dedicated SSL VPN Tunnel	
Click the button to enable the dedicated SSL VPN tunnel function. This way, you can access only the internal network resources specified in the tunnel routing but not Internet resources after you log in to SSL VPN.  **Notes:** • The client versions that support the dedicated SSL VPN tunnel function include: the latest version of the SSL VPN client for Windows, the latest version of the SSL VPN client for macOS, and the latest version of the SSL VPN client for Linux. • The dedicated SSL VPN tunnel function cannot be used together with the domain route function.	

Tunnel Route

- After you enable the dedicated SSL VPN tunnel function, we recommend that you do not configure a default route in the tunnel routing.

Enable Domain Route

Specifies the destination domain name that you want to access through SSL VPN tunnel.

After clicking the **Enable** button, system will distribute the specified domain names to the VPN client, and the client will generate the route to the specified destination according to the resolving results from the DNS.

Notes: The domain route function cannot be used together with the dedicated SSL VPN tunnel function.

Maximum	The maximum numbers of routes that can be generated after obtaining the resolved IP addresses of the domain name. The value ranges from 1 to 10000. The default value is 1000.
New	Click **New** to add the domain name to the list and you can add up to 64 domain names.
Domain	Specifies the URL of the domain name. The URL cannot exceed 63 characters and it cannot end with a dot (.). Both wildcards and a single top level domain, e.g. **com** and **.com** are not supported.
Delete	Click **Delete** to delete the selected domain name.

In the Binding Resource tab, configure the binding relationship between user groups, roles and resources.

Binding Resource	
New	Click **New** to add binding entries for resources and user groups, roles to the list below. You can repeat to add more items.
Name	Select an existing resource name from the drop-down list. The range is 1 to 63 characters.
Type	Select the binding type from the drop-down list. It can be a type of user group or role.
Resource List	Select an existing resource name from the drop-down list. The range is 1 to 63 characters.
User Group/role	Select an existing user group/role from the drop-down list. Click  to add a user group or a role. Select the AAA servers where user groups reside from the drop-down list. Currently, only the local authentication server and the RADIUS server are available. **Note**: • A user group/role can be bound with multiple resources, and a resource can also be bound with multiple user groups/roles. • Only 256 binding entries can be configured in an SSL VPN instance.
AAA Server	Select the AAA servers where user groups reside from the drop-down list. Currently, only the local authentication server and the RADIUS server are available.

Binding Resource	
Delete	Click **Delete** to delete the selected item.

3. If necessary, click **Advanced Configuration** to configure the advanced functions, including parameters, client, host security, SMS authentication, and optimized path.

In the Parameters tab, configure the corresponding options.

Security Kit	
SSL Version	Specifies the SSL protocol version. The default is TLSv1.2. **Any** indicates one of TLSv1, TLSv1.1, TLSv1.2, TLSv1.3 protocol will be used. If tlsv1.2 or any is specified to the SSL protocol in SSL VPN server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the tlsv1.2 protocol before the digital certificate authentication via SSL VPN client, so that the SSL VPN server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate. We will take the certificate file named oldcert.pfx as an example, the procedure is as follows: 1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format. **openssl pkcs12 –in oldcert.pfx –out cert.pem** 2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that

Security Kit	
	supports tlsv1.2 protocol. **openssl pkcs12 –export –in cert.pem –out new-cert.pfx –CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"** 3. Import the newly generated .pfx format certificate into your browser or USB Key. After the above operation, you have to log into SSL VPN server with SSL VPN client whose version is 1.4.6.1239 or later.
Trust Domain	Specifies the trust domain. When the GMSSLv1.0 protocol is used, the specified PKI trust domain needs to include the SM2 signature certificate and its private key for the GMSSL negotiation.
Encryption Trust Domain	When using the GMSSLv1.0 protocol, you must config this option. The specified encryption PKI trust domain needs to include the SM2 encryption certificate and its private key for the GMSSL negotiation.
Encryption	Specifies the encryption algorithm of the SSL VPN tunnel. The default value is AES. **NULL** indicates no encryption. When using the GMSSLv1.0 protocol, you're recommended to select SM4 for the encryption algorithm.
Hash	Specifies the hash algorithm of the SSL VPN tunnel. The default value is MD5. **NULL** indicates no hash. When using the GMSSLv1.0 protocol, you're recommended to select SM3 for the hash algorithm.
Compression	Specifies the compression algorithm of the SSL VPN tun-

Security Kit	
	nel. By default, no compression algorithm is used.
Client Connection	
Allow Download Client from Browser	Select the check box of the client type to specify the allowed type of SSL VPN client. By default, you are allowed to access the system with five types of SSL VPN clients, which are SSL VPN client for Windows, SSL VPN client for Android, SSL VPN client for iOS, SSL VPN client for macOS, and SSL VPN client for Linux. You can configure to access the system only via the specified types of SSL VPN clients as needed.
Idle Time	Specifies the time that a client stays online without any traffic with the server. After waiting for the idle time, the server will disconnect from the client. The value range is 1 minute to 25 hours. The default value is 30 minutes.
Forced Logoff Schedule	Specifies the forced logoff schedule from the drop-down list. When the schedule takes effect, the system forces online SSL VPN users to log out based on the periodic schedule or the timeframe. Note: • The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect. • SSL VPN users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.
Multiple Login	This function permits one client to sign in more than one place simultaneously. Select the **Enable** check box to enable the function.
Multiple	Type the number of simultaneous login with the same user

Security Kit	
Login Times	name into the **Multiple Login Times** box. The value range is 0 to 99,999,999. The value of 0 indicates no limitation. The default value is 0.
Advanced Parameters	
Anti-Replay	The anti-replay function is used to prevent replay attacks. The default value is 32.
DF-Bit	Specifies whether to permit packet fragmentation on the device forwarding the packets. The actions include: • Set - Forbids packet fragmentation. • Copy - Copies the DF value from the destination of the packet. It is the default value. • Clear - Permits packet fragmentation.
Port (UDP)	Specifies the UDP port number for the SSL VPN connection. The value range is 1 to 65535.
Port (TCP)	Specifies the TCP port number for the SSL VPN connection. The value range is 1 to 65535.

In the Client tab, configure the corresponding options.

Client Configuration	
Allowed Client Types	Select one or more client types. By default, the system allows all of the 6 types of SSL VPN clients to access: the SSL VPN client for Windows, the SSL VPN client for Android, the SSL VPN client for iOS, the SSL VPN client for macOS, the SSL VPN client for Linux, and the SSL VPN client for ChineseOS. You can configure a specified allowed type of SSL VPN client as required.

Client Configuration	
Change Password URL	Specifies the URL address that can redirect to the specified URL page from the client to modify the password. The length is 0 to 255 characters.
Forgot Password URL	Specifies the URL address that can redirect to the specified URL page from the client to reset the password. The length is 0 to 255 characters. **Notes:** This configuration takes effect only after Change Password function is enabled on the local server.
Redirect URL	This function redirects the client to the specified redirected URL after a successful authentication. Type the redirected URL into the box. The value range is 0 to 255 characters. HTTP (http://) and HTTPS (https://) URLs are supported. Based on the type of the URL, the corresponding fixed format of URL is required. Take the HTTP type as the example: • For the UTF-8 encoding page - The format is URL+username=$USER&password=$PWD, e.g., http://www.-abc.-com/oa/-login.do?username=$USER&password=$PWD • For the GB2312 page - The format is URL+username=$GBUSER&password=$PWD, e.g., http://www.-abc.-com/oa/-

Client Configuration	
	login.do?username=$GBUSER&password=$PWD • Other pages: - Type the URL directly, e.g., http://www.abc.com
Title	Specifies the description for the redirect URL. The value range is 0 to 31 characters. This title will appear as a client menu item.
Delete privacy data after dis-connection	Select **Enable** to delete the corresponding privacy data after the client's disconnection.
Digital Certificate Authentication	
Authentic-ation	Click **Enable** to enable this function. There are two options available: • Username/Password + Digital Certificate - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate, and also type the correct username and password. The USB Key certificate users also need to type the USB Key password. • Digital Certificate only - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate. The USB Key certificater users also need to type the USB Key password. No username or user's password is required.

Client Configuration	
	When **Digital Certificate only** is selected: • System can map corresponding roles for the authenticated users based on the CN or OU field of the USB Key certificate. For more information about the role mapping based on CN or OU, see "Role" on Page 976. • System does not allow the local user to change the password. • System does not support SMS authentication. • The client will not re-connect automatically if the USB Key is removed.
USB KEY Download URL	When USB Key authentication is enabled, you can download the UKey driver from this URL. The length is 0 to 63 characters.
Trust Domain Subject&Username Checking CN Matching OU Matching	To configure the trust domain and the subject & username checking function: 1. From the Trust domain drop-down list, select the PKI trust domain that contains the CA (Certification Authority) certificate. If the client's certificate is the only one that matches to any CA certificate of the trust domain, then the authentication will succeed. 2. If necessary, select the **Subject&Username Checking** check box to enable the subject & username

Client Configuration	
	check function. After enabling it, when the user is authenticated by the USB Key certificate, system will check whether the subject CommonName in the client certificate is the same as the name of the login user. You can also enter the strings in the **CN Match** box and the **OU** box to determine whether matches them. 3. Click **Add**. The configured settings will be displayed in the list below. To delete an item, select the item you want to delete from the list, and then click **Delete**.

In the Two-Step verification tab, configure the corresponding options.

Option	Description
Two-Step Verification	Click **Two-Step Verification** to enable the function. Two-Step Verification means that when an SSL VPN user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS Authentication, Token Authentication or Email Authentication after the username and password is entered. The user must enter the random verification code received in order to log into SSL VPN and access intranet resources.
Type	Specifies the type of Two-Step Verification, including SMS Authentication, Token Authentication and Email Authentication:

Option	Description
	• SMS Authentication: Click **SMS Modem** or **SMS Gateway** to specify the authentication type, and configure corresponding options below as needed. • Token Authentication: Enter prompt message as needed. The length is 0 to 255 characters. • Email Authentication: Configure corresponding options below as needed.
SMS Authentication	
SMS Authentication	Select the **SMS Authentication** to enable the function. And select the **SMS Modem** or **SMS Gateway** to specify the SMS authentication type.
SMS Gateway Name	Select the SMS gateway name from drop-down list. For more information about SMS Gateway, see "SMS Gateway" on Page 1815.
Lifetime of SMS Verification Code	Specifies the lifetime of the SMS authentication code. The range is 1 to 10 minutes. The default value is 10.
Sender Name	Specifies a message sender name to display in the message content. The range is 0 to 63 characters. **Notes:** Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enter-

Option	Description
	prise information platform.
Verification Code Length	Specifies the length of the SMS verification code. The value range is 4 to 8. The default value is 8. Note: If a ChinaMobileMusic service provider name is specified for the "SMS Gateway Name" option, the range of the length of the SMS verification code is 4 to 6.
SMS Template	Specifies the SMS verification content. The input must contain " $ VRFYCODE" (This parameter is used to get the verification code). "$USERNAME" and "EXPIRATION" are optional. The value range is 9 to 500 characters. Note: If a ChinaMobileMusic service provider name is specified for the "SMS Gateway Name" option, the content of text messages must be " $ VRFYCODE".
Sign Name	If an ALIYUNSMS service provider name is specified for the "SMS Gateway Name" option, the sign name must be entered in this field and will be displayed in the message content. The range is 1 to 63 characters. This parameter should be the same with the sign name applied in the SMS of Alibaba Cloud.
Template Code	If an ALIYUNSMS service provider name is specified for the "SMS Gateway Name" option, the code of the SMS template must be entered in this field. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the SMS of Alibaba Cloud.

Option	Description
Email Authentication	
Mail Server	Specifies the existing Email server which the Email address that used to send the verification code is configured on. The range is 1 to 31 characters. For more information about the configuration of Mail Server, see "Mail Server" on Page 1812.
Lifetime of Email Verification Code	Specifies the lifetime of the Email verification code. The range is 1 to 10 minutes. The default value is 10. Each Email verification code has a period of validity. If the user neither types the verification code within the period nor applies for a new code, SSL VPN server will disconnect the connection.
Sender Name	Specifies a verification code sender name to display in the Email content. The range is 0 to 63 characters. In order to prevent the mail from being identified as spam, it's recommended that users to configure the sender name.
Verification Code Length	Specifies the length of the Email verification code. The value range is 4 to 8. The default value is 8.
Email Verification Content	Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The length is 18 to 128 characters. The default content is "SSL VPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.".

In the Host Compliance Check/Binding tab, configure the corresponding options.

Host Compliance Check	
Creates a host compliance check rule to perform the host compliance check function. Before creating a host compliance check rule, you must first configure the host compliance check profile in "Configuring a Host Compliance Check Profile" on Page 635.	
Role	Specifies the role to which the host compliance check rule will be applied. Select the role from the **Role** drop-down list. **Default** indicates the rule will take effect to all the roles.
Host Compliance Check	Specifies the compliance check profile. Select the profile from the **Host Compliance Check** drop-down list.
Exception handling method	Specifies the exception handling method. • Guest Role: Select the guest role from the **Guest Role** drop-down list. The user will get the access permission of the guest role when the host checking fails. If —— is selected, system will disconnect the connection when the host compliance check fails. • Redirect URL: Click the **Redirect URL** radio button, and then type the URL into the textbox. When the host checking fails, the browser jump to the specified URL and guide the user to download the software required for host security detection and disconnect the client. If this option is not configured, the client will be disconnected.

Host Compliance Check	
Guest Role	Select the guest role from the **Guest Role** drop-down list. The user will get the access permission of the guest role when the host checking fails. If **Null** is selected, system will disconnect the connection when the host compliance check fails.
Periodic Check	Specifies the host compliance check period. System will check the status of the host automatically according to the host compliance check profile in each period.
Add	Click **Add**. The configured settings will be displayed in the table below.
Delete	To delete an item, select the item you want to delete from the list, and then click **Delete**.
Host Binding	
Enable Host Binding	Click **Enable** to enable is this function. By default, one user can only log in one host. You can change the login status by configuring the following options. • Allow one user to login through multiple hosts. • Allow multiple users to login on one host. • Automatically add the user-host ID entry into the binding list at the first login. **Note**: To use the host binding function, you still have to configure it in the host binding configuration page. For more information about host binding, see "Host Binding" on Page 628.

In the Optimized Path tab, configure the corresponding options.

Option	Description
Optimal path detection can automatically detect which ISP service is better, giving remote users a better user experience.	
No Check	Do not detect.
Client	The client selects the optimal path automatically by sending UDP probe packets.
The device	When the client connects to the server directly without any NAT device, this is the detection process: 1. The server recognizes the ISP type of the client according to the client's source address. 2. The server sends all of the sorted IP addresses of the egress interfaces to the client. 3. The client selects the optimal path. When the client connects to the server through a NAT device, this is the detection process: 1. The server recognizes the ISP type of the client according to the client's source address. 2. The server sends all of the sorted NAT IP addresses of the external interfaces to the client. 3. The client selects the optimal path.
NAT Mapping Address and Port	If necessary, in the NAT mapping address and port section, specify the mapped public IPs and ports of the server referenced in the DNAT rules of the DNT device. When the client connects to the server through the

Option	Description
	DNAT device, the NAT device will translate the destination address of the client to the server's egress interface address. Type the IP address of the NAT device's external interface and the HTTPS port number (You are not recommended to specify the HTTPS port as 443, because 443 is the default HTTPS port of WebUI management). You can configure up to 4 IPs.

4. Click **Done** to save the settings.

To view the SSL VPN online users, take the following steps:

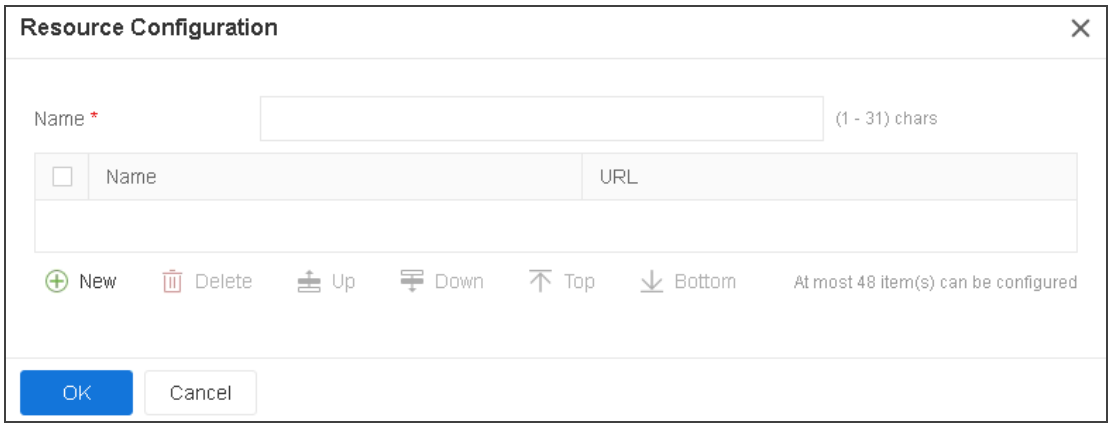
1. Select **Configure > Network > SSL VPN**.
2. Select an SSL VPN instance.
3. View the detailed information of the online users in the table. You can also click Filter to add filter conditions (Online Users, User group, Host Binding ID) to view the detailed information of SSL VPN online users that meet the filter conditions.

Configuring Resource List

Resource list refers to resources configured in system that can be easily accessible by users. Each resource contains multiple resource items. The resource item is presented in the form of a resource name followed by resource item name in your default browser page. After the SSL VPN user is authenticated successfully, the authentication server will send the user group information of the user to the SSL VPN server. Then, according to the binding relationship between the user group and resources in the SSL VPN instance, the server will send a resource list in which the user can access to the client. After that, the client will analyze and make the default browser in system pop up a page to display the received resource list information, so that the user can access the private network resource directly by clicking the resource item name. The resource list page pops up only after the authentication is passed. If a user does not belong to any user group, the browser will not pop up the resource list page unless authentication is passed.

To configure resource list for SSL VPN:

1. Select **Network > VPN > SSL VPN**.
2. Click **Configuration > Resources List** at the top-right corner.
3. Click **New**.



Option	Description
Name	Enter a name for the new resource. The range is 1 to 63 characters.
Resource Item	
Name	Enter a name for a new resource item. Names of resource items in different resources can not be the same. The range is 1 to 95 characters
URL	Enter a URL for a new resource item.
Add	Click **Add**to add this binding item to the list below. **Note**: The maximum configurable resourse entries of different platforms vary in three levels: 200 entries, 500 entries, and 1000 entries.
Delete	To delete a rule, select the rule you want to delete

Option	Description
	from the list and click **Delete**.
Up/Down/Top/Bottom	You can move the location for items at your own choice to adjust the presentation sequence accordingly.

4. Click **OK**, the new resource will be displayed in the resource list.

   At most 3 resource items can be displayed in the resource list for each resource, and the other items will be displayed as "...". You can click **Edit** or **Delete** button to edit or delete the selected resource.



Notes:

- Less than 256 resource lists can be configured.
- The maximum number of resource entries that can be configured on different platforms is different. Please refer to the actual situation.
- SSL VPN client versions that allow you to configure the resource list are as follows: SSL VPN client 5.0.0 or later version (including Windows/macOS/Linux/iOS /Android/macOS/ChineseOS).

Host Binding

The host binding function verifies that the hosts are running the SSL VPN clients according to their host IDs and user information. The verification process is:

1. When an SSL VPN user logs in via the SSL VPN client, the client will collect the host information of main board serial number, hard disk serial number, CUP ID, and BIOS serial

number.

2. Based on the above information, the client performs the MD5 calculation to generate a 32-digit character, which is named host ID.
3. The client sends the host ID and user/password to the SSL VPN server.
4. The SSL VPN server verifies the host according to the entries in the host unbinding list and host binding list, and deals with the verified host according to the host binding configuration.

The host unbinding list and host binding list are described as follows:

- Host unbinding list: The host unbinding list contains the user-host ID entries for the first-login users.
- Host binding list: The host binding list contains the user-host ID entries for the users who can pass the verification. The entries in the host unbinding list can be moved to the host binding list manually or automatically for the first login. When a user logs in, the SSL VPN server will check whether the host binding list contains the user-host ID entry of the login user. If there is a matched entry in the host binding list, the user will pass the verification and the sever will go on checking the user/password. If there is no matched entry for the login user, the connection will be disconnected.

Note: For hosts deployed on virtual platforms, the host ID might not be unique. Therefore, the host binding function might not work properly.

Configuring Host Binding

Configuring host binding includes host binding/unbinding configurations, super user configurations, shared host configurations, and user-host binding list importing/exporting.

Configuring Host Binding and Unbinding

To add a binding entry to the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Compliance Check-/Binding page.
1. With the Binding and Unbinding tab active, select the entries you want to add to the Host Unbinding List. You can also click 

to add filter conditions (User, Host ID) to view the detailed information of entries that meet the filter conditions.
2. Click **Add** to add the selected entries to the Host Binding List.

To delete a binding entry from the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Compliance Binding page.
3. With the Binding and Unbinding tab active, select the entries you want to delete from the Host binding List. You can also click 

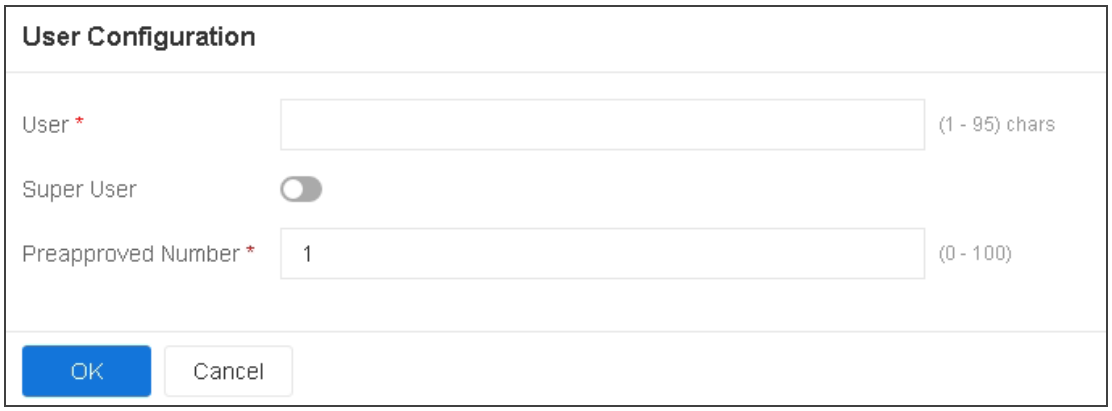
to add filter conditions (User, Host ID) to view the detailed information of entries that meet the filter conditions.
4. Click **Unbinding** to remove the selected entries from this list.

Configuring a Super User

The super user won't be controlled by the host checking function, and can log into any host. To configure a super user, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Binding page.

3. With the User Privilege List tab active, click **New**.



Option	Description
User	Specifies the name of the user. The length is 1 to 95 characters.
Super User	Select the **Enable** check box to make it a super user.
Preapproved Number	If system allows one user to login from multiple hosts, and the option of automatically adding the user-host ID entry into the host binding list at the first login is enabled, then by default system only records the user and first login host ID entry to the host binding list. For example, if the user logs in from other hosts, the user and host ID will be added to the host unbinding list. This pre-approved number specifies the maximum number of user-host ID entries for one user in the host binding list.

4. Click **OK** to save the settings.

Configuring a Shared Host

Clients that log in from the shared host won't be controlled by the host binding list. To configure a shared host, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Binding page.
3. With the Host ID Privilege List tab active, click **New**.



Option	Description
Host ID	Type the host ID into the Host ID box.
Shared Host	Select the **Enable** check to make it a shared host. By default, this check box is selected.

4. Click **OK** to save the settings.

Importing/Exporting Host Binding List

To import the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Binding page.
3. With the Binding and Unbinding tab active, click **Import**.
4. Click **Browse** to find the binding list file and click **Upload**.

To export the host binding list, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Host Compliance Binding** to visit the Host Checking/Binding page.

3. With the Binding and Unbinding tab active, click **Export**.

4. Select a path to save the host binding list.

Host Compliance Check

The host compliance check function checks the security status of the hosts running SSL VPN clients, and according to the check result, the SSL VPN server will determine the security level for each host and assign corresponding resource access right based on their security level. It a way to assure the security of SSL VPN connection. The checked factors include the operating system, IE version, and the installation of some specific software.

The factors to be checked by the SSL VPN server are displayed in the list below:

Factor	Description
Operating system	• Operating system, e.g., Windows 2000, Windows 2003, Windows XP, Windows Vista, Windows 7m Windows 8, etc. • Service pack version, e.g., Service Pack 1 • Windows patch, e.g., KB958215, etc.
	• Whether the Windows Security Center and Automatic Updates are enabled. • Whether the installation of AV software is compulsory, and whether the real-time monitor and the auto update of the signature database are enabled. • Whether the installation of anti-spyware is compulsory, and whether the real-time monitor and the online update of the signature database are enabled. • Whether the personal firewall is installed, and whether the real-time protection is enabled.
	Whether the IE version and security level reach the specified requirements.

Factor	Description
Other configurations	Whether the specified processes are running.
	Whether the specified services are installed.
	Whether the specified services are running.
	Whether the specified registry key values exist.
	Whether the specified files exist in the system.

Role Based Access Control and Host Compliance Check Procedure

Role Based Access Control (RBAC) means that the permission of the user is not determined by his user name, but his role. The resources can be accessed by a user after the login is determined by his corresponding role. So role is the bridge connecting the user and permission.

The SSL VPN host checking function supports RBAC. And the concepts of primary role and guest role are introduced in the host checking procedure. The primary role determines which host compliance check profile (contains the host checking contents and the security level) will be applied to the user and what access permission can the user have if he passes the host checking. The guest role determines the access permissions for the users who fail the host checking.

The host compliance check procedure is shown as below

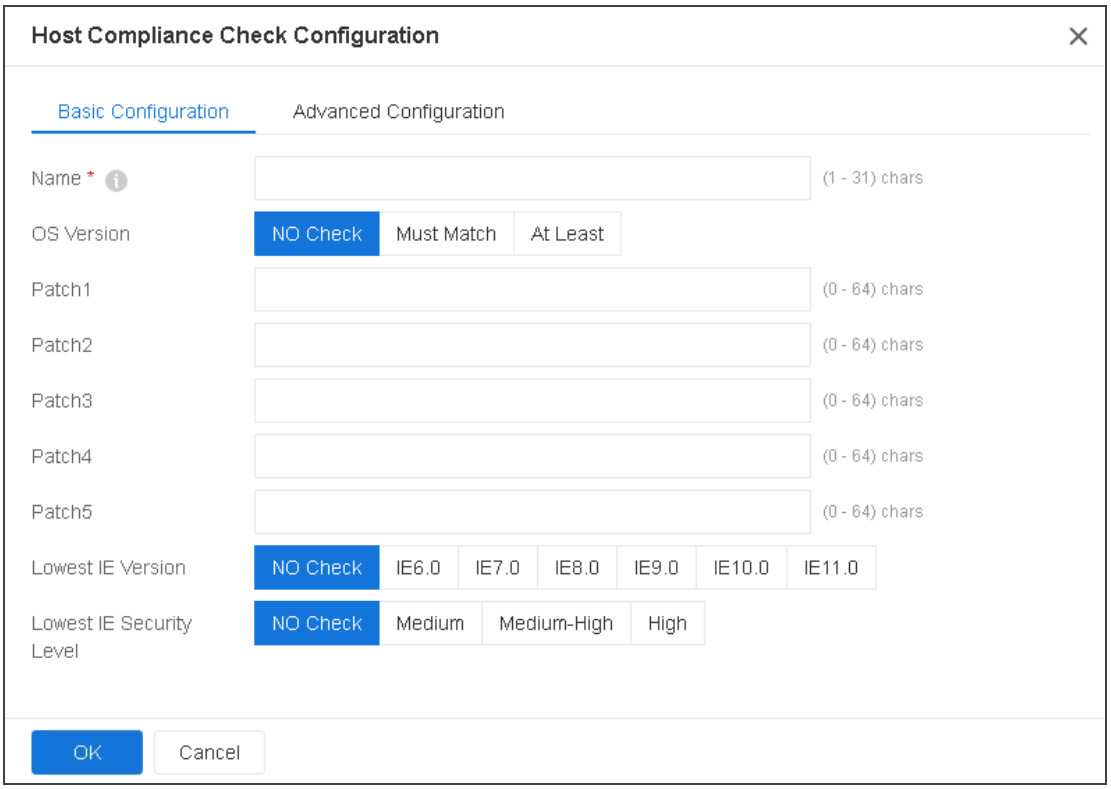
1. The SSL VPN client sends request for connection and passes the authentication.
2. The SSL VPN server sends the host checking profile to the client.
3. The client checks the host security status according to the items in the host checking profile. If it fails the host compliance check, system will be notified of the checking result.
4. The client sends the checking result back to the server.
5. The server disconnects the connection to the failed client or gives the guest role's access permission to the failed client.

The host compliance check function also supports dynamic access permission control. On one side, when the client's security status changes, the server will send a new host checking profile to the client to make him re-check; on the other side, the client can perform security checks periodically. For example, if the AV software is disabled and is detected by the host checking function, the role assigned to the client may change as will the access permissions.

Configuring a Host Compliance Check Profile

To configuring host compliance check profile, take the following steps:

1. Select **Network > VPN > SSL VPN**.
2. At the top right corner, click **Configuration** ,select **Host Compliance Check** from the drop-down list to visit the Host Compliance Check page.
3. In the Host Compliance Check tab, click **New** to create a new host checking rule.



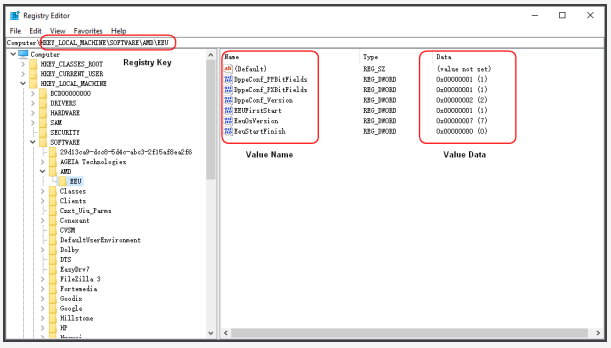
In the Basic Configuration tab, configure the corresponding options.

Option	Description
Name	Specifies the name of the host checking profile.
OS Version	Specifies whether to check the OS version on the client host. Click one of the following options: • No Check: Do not check the OS version. • Must Match: The OS version running on the client host must be the same as the version specified here. Select the OS version and service pack version from the drop-down lists respectively. • At Least: The OS version running on the client host should not be lower than the version specified here. Select the OS version and service pack version from the drop-down lists respectively.
Patch1/2/3/4/5	Specifies the patch that must be installed on the client host. Type the patch name into the box. Up to 5 patches can be specified.
Lowest IE Version	Specifies the lowest IE version in the Internet zone on the client host. The IE version running on the client host should not be lower than the version specified here.
Lowest IE Security Level	Specifies the lowest IE security level on the client host. The IE security level on the host should not be lower than the level specified here.

In the Advanced Configuration tab, configure the corresponding options.

Option	Description
Security Center	Checks whether the security center is enabled on the client host.

Auto Update	Checks whether the Windows auto update function is enabled.
Anti-Virus Software	Checks the status and configurations of the anti-virus software: • Installed: The client host must have the AV software installed. • Monitor: The client host must enable the real-time monitor of the AV software. • Virus Signature DB Update: The client host must enable the signature database online update function.
Anti-Spyware Software	Checks the status and configurations of the anti-spyware software: • Installed: The client host must have the anti-spyware installed. • Monitor: The client host must enable the real-time monitor of the anti-spyware. • Signature DB Update: The client host must enable the signature database online update function.
Firewall	Checks the status and configurations of the firewall: • Installed: The client host must have the personal firewall installed. • Monitor: The client host must enable the real-

	time monitor function of the personal firewall.
Registry Key Value	
Key1/2/3/4/5	Checks whether the registry key, value name, and value data exists. Up to 5 registry keys values can be configured. The check types are: • No Check: Do not check the registry key, value name, and value data. • Exist: The client host must have the registry key, value name, and value data. Type the registry key, value name, and value data into the boxes, as shown in the following figure:  • Do not Exist: The client cannot have the registry key, value name, and value data. Type the registry key, value name, and value data into the boxes, as shown in the above figure. **Note**: If you enter a field, all fields before this field are required. For example, if you enter the value data, the registry key and value name are required.
File Path Name	
File1/2/3/4/5	Checks whether the file exists. Up to 5 files can be

	configured. The check types are: • No Check: Do not check file. • Exist: The client host must have the file. Type the value into the box. • Do not Exist: The client cannot have the file. Type the value into the box.
Name of Running Process	
Process1/2/3/4/5	Checks whether the process is running. Up to 5 processes can be configured. The check types are: • No Check: Do not check the process. • Exist: The client host must have the process run. Type the process name into the box. • Do not Exist: The client cannot have the process run. Type the process name into the box.
Name of Installed Service	
Service1/2/3/4/5	Checks whether the service is installed. Up to 5 services can be configured. The check types are: • No Check: Do not check the service. • Exist: The client host must have the service installed. Type the service name into the box. • Do not Exist: The client host cannot have the service installed. Type the service name into the box.

Name of Running Service	
Service1/2/3/4/5	Checks whether the service is running. Up to 5 services can be configured. The check types are: • No Check: Do not check the service. • Exist: The client host must have the service run. Type the service name into the box. • Do not Exist: The client host cannot have the service run. Type the service name into the box.

4. Click **OK** to save the settings.

Secure Connect Client Management

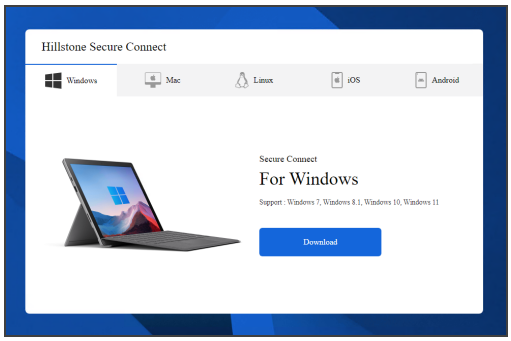
End users can download Secure Connect clients at the following addresses:

- Client download address on the device: https://IP-Address:Port-Number. The "IP-Address" and "Port-Number" refer to the IP address of the egress interface and HTTPS port number specified in the configuration of the SSL VPN or ZTNA instance.
- Client download address provided by Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.
- To download and install Hillstone Secure Connect client for ChineseOS, search for "Hillstone Secure Connect" in the APP Store that comes with ChineseOS.

By default, the two addresses on the device and on the official website of Hillstone Networks use the same download source, and the downloaded Secure Connect client is also the same.

Customizing Secure Connect Download Page

You can customize the title and background of the download address on the device. The default download page is shown as below:



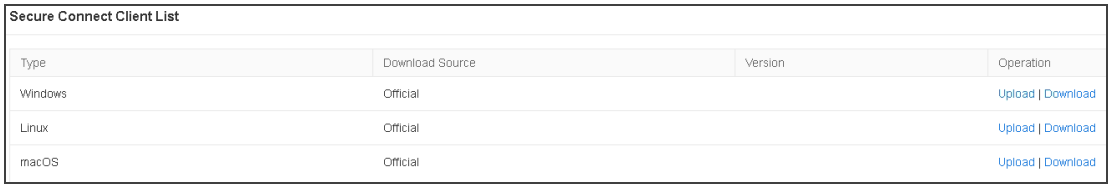
To customize the Secure Connect download page, take the following steps:

1. Select **System > Secure Connect Client Management**.
2. In the "Configure Secure Connect Client Download Page" area, click **Upload Background Picture > Browse** to select the background picture. The picture needs to be PNG format. The recommended resolution is 1920px*1080px. The size cannot exceed 2MB.
3. Click **Upload** to upload the background picture to system. After uploading successfully, you will have completed the background picture modification.
4. Enter the title in the **Download Page Tittle** box to customize the title of the download page. The length is 1 to 63 characters.
5. Click **OK** to save the settings. Clicking **Cancel** will only affect the authentication page title modification.

If you want to restore the default picture, click **Restore Default Background** . Then click **OK**.

Customizing Client Download Source

By default, the client download source on the device is the same with that on Hillstone Networks Official Website. In the application scenario where you want end users to download and use specific Secure Connect clients, such as a client of the specified version or a customized client, you can import the client into the system to overwrite the default download source on the device. You can import Windows, macOS and Linux type clients.



To import the client, take the following steps:

1. Select **System > Secure Connect Client Management**.
2. In the "Secure Connect Client List" area, locate the type of client to be imported and click **Upload**.
3. In the "Upload Secure Connect Client for Windows/macOS/Linux" dialog box, click **Browse** and select the client file to be imported, and click **Upload**. The file name should be in the "xxx_version_check.exe/run/dmg/pkg" format. "xxx" indicates the file name; "version"indicates the client version, starting with the letter "v"; "exe" is the extension for Windows type client file; "run" is the extension for Linux type client file; "dmg" and "pkg" are the extensions for macOS type client file. The file size cannot exceed 100MB. An example is "secure-connect_v1.4.9.2000_1a6755fe.exe".
4. After uploading, the download source for this client will change from "Offical" to "Local" in the "Secure Connect Client List".
5. Click **Download** to check the downloaded client is the imported one.

6. Click **Delete** to delete the imported client. After the imported client is deleted, the download source will be resorted to "Official".

Hillstone Secure Connect Client for Windows

The SSL VPN/ZTNA client for Windows is Hillstone Secure Connect. It can run in the following operating systems:

- Windows7 SP1/Windows8.1/Windows10/Windows11
- Windows server 2008 R2/Windows server 2012/Windows server 2012 R2/Windows server 2016/Windows server 2019/Windows server 2022

The encrypted data can be transmitted between the client and the device after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC on which the client is running.
- Show the connecting status, statistics, interface information, and route information.
- Show log messages.
- Upgrade the client software.
- Resolve the resource list information received from the server.
- Collect and report endpoint device status information.

System supports IPv4 and IPv6 Secure Connect Windows clients.

This section mainly describes how to download, install, start, uninstall the Secure Connect Windows client, and gives instructions on how to use its GUI and menu. The device side supports the following authentication methods:

- Username/Password
- Username/Password + Digital Certificate (including USB Key certificate and file certificate)

- Digital Certificate (including USB Key certificate and file certificate) only
- Third-party Application Login (OAuth2 authentication)

System supports IPv4 and IPv6 Secure Connect Windows clients.

Downloading and Installing the Client

Take either of the following methods to download and install the Secure Connect Windows client:

- Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.
- Visit https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.

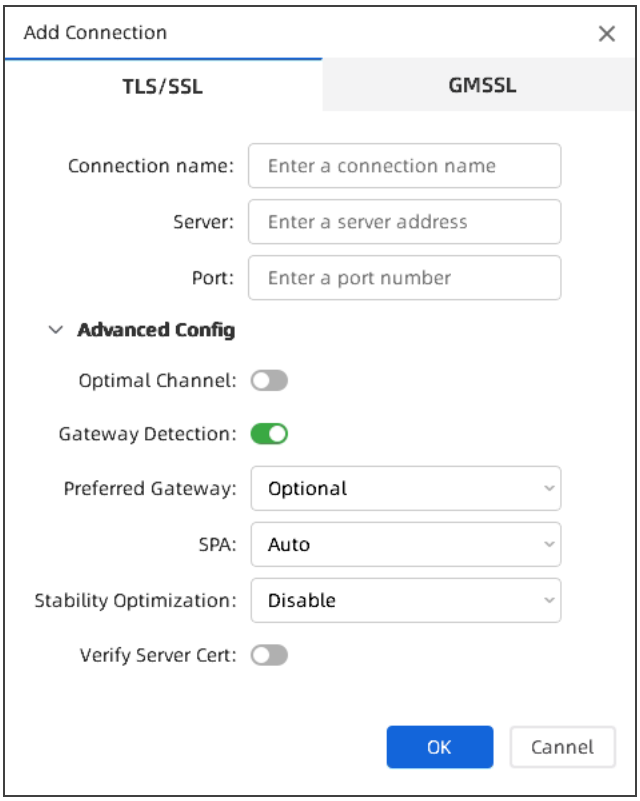
A virtual network adapter will be installed on your PC together with the Secure Connect Windows client. It is used to transmit encrypted data between the device and the client.

Starting Up and Connecting

After the Secure Connect Windows client is installed successfully, take the following steps to start and log in the client:

1. Double-click the shortcut of Hillstone Secure Connect on your desktop, or from the Start menu, choose **All Programs > Hillstone Secure Connect > Hillstone Secure Connect**. The client main page is displayed.

2. Click **Add Connection**. The following dialog box is displayed.



Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
GMSSL	Select this tab to use the GMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Advanced Config: By default, advanced configurations are hidden. You can click › to expand this section and configure the following options.	

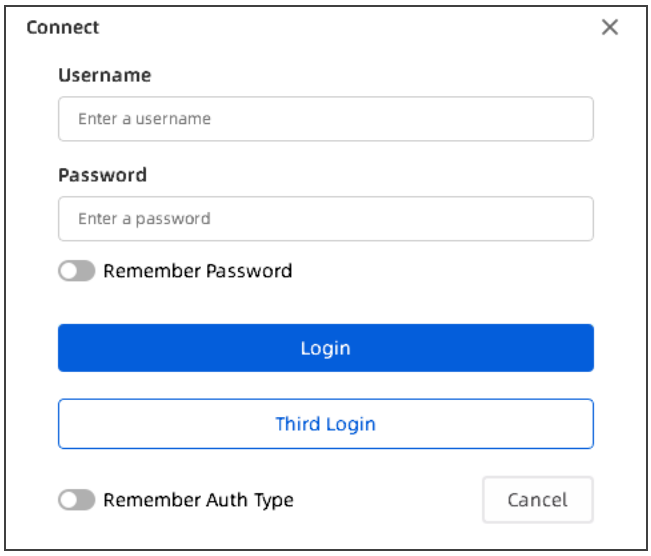
Option	Description
Optimal Channel	Set whether to enable optimal path detection function. This function is used for the SSL VPN access function. When the optimal path detection is enabled on both the device and the client, clients connected from different ISP lines can automatically choose the fastest route to connect to the device of SSL VPN. By default, this function is disabled.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.

Option	Description
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.
Verify Server Cert	Click **Enable** button to verify the certificate of the server when establishing the connection. To add trusted certificates, please refer to General Configuration.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.

4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. On the Connect dialog box, select an authentication type. The client will attempt to establish a connection to the device.

   The authentication type includes username/password, username/password+certificate, certificate, and third-party application login. If the access user on the device selects an OAuth2 server, OAuth2 authentication will be used as the third-party application login. In this case, you will be redirected to the OAuth2 authentication process: click the OAuth2 authentication icon, enter the OAuth2 authentication page, the browser will return the authentication result after the OAuth2 authorization and authentication complete, and a login status will be returned to the client.



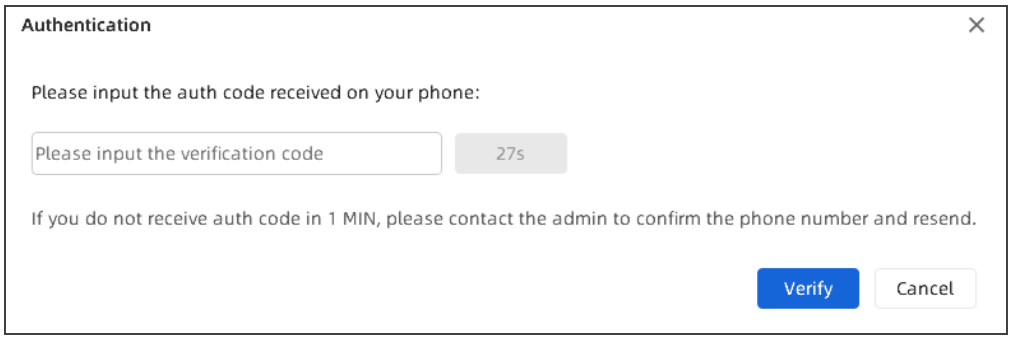
Option	Description
Username	Enter the name of the login user. When Auth type is specified as "Username" or "Username + Certificate", the client user name and password should be entered.

Option	Description
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Certificate	When the authentication type is "Username + Certificate" or "Certificate", click this option to enter the dialog box for selecting a certificate. The selected certificate will be sent to the device for authentication.
Select Digital Certificate	Options in the "Select Digital Certificate" dialog box are described as follows: • Default System Certificate: Click this radio button to allow the device to use the Hillstone UKey certificate as the system default certificate. This is the default setting. • USBKey Certificate: Click this radio button and select a USB-Key certificate from the current certificate list. The USB Key should be inserted into the USB interface of the PC in advance. You can use the USB Key deployment tool named SelectUSBKey to set the third-party certificate as the default certificate. For more information, refer to Third-Party USB Key. • File Certificate: Click this radio button and select a file certificate from the current certificate list. The file certificate should be imported into the PC in advance. • Certificate list: Display the existing certificate in the system. Click **Refresh** icon to update the list.

Option	Description
GMSSL certificate	Options in the "GMSSL certificate" dialog box are described as follows: • Device Name: Select the current USB Token device name in the drop-down list. The USB Token device should be inserted into the USB interface of the PC in advance. • Application Name: The application is a structure that contains a container, a device authentication key, and a file. Select the specified application name in the drop-down list. • Container Name: The container is the unique storage space in the USB Token device to save the key. It is used to store the encryption key pair, the encryption certificate corresponding to the encryption key pair, the signature key pair, and the signature certificate corresponding to the signature key pair. Select the name of the specified container in the drop-down list. • Signature certificate: Display the name of the SM2 signature certificate in the specified container. • Encryption certificate: Display the name of the SM2 encryption certificate in the specified container.
PIN	Enter the PIN code of the USB Key when the authentication type is "User name/Password + Digital certificate" or "Only

Option	Description
	Digital certificate".
Remember PIN	After this option is enabled, you do not need to enter the PIN at the next-time connection.
Remember Password	After this option is selected, you do not need to enter the user's password at the next-time connection.
Remember Auth Type	after this option is selected, this authentication type will be directly used upon next connection. By default, this option is selected. If you disable this function, you need to select an authentication type again upon next connection. **Note**: When the authentication type on the device changes, if the remembered authentication type is not included in the changed authentication type, you will be prompted that the authentication type is different from that on the device upon your next connection. In this case, you need to select an authentication type again.

5. If SMS authentication is enabled, type the authentication code into the box in the SMS Auth dialog (as shown below) and click **Verify**. If you have not received the authentication code within one minute, you can re-apply by clicking **Resend**.



6. If token authentication is enabled on the device side, the token Authentication dialog will appear. You need to pass the token authentication.

    - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
    - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.

7. If Email authentication is enabled on the device side, the Email Authentication dialog will appear. You need to pass the Email authentication.

    - After passing the authentication, you have three chances to type the authentication code. If you give incorrect authentication code three times in succession, the connection will be disconnected automatically.
    - You have three chances to apply the authentication code, and the sending interval is one minute. Re-applying authentication code will void the old code, thus you must provide the latest code to pass the authentication.



Tips:

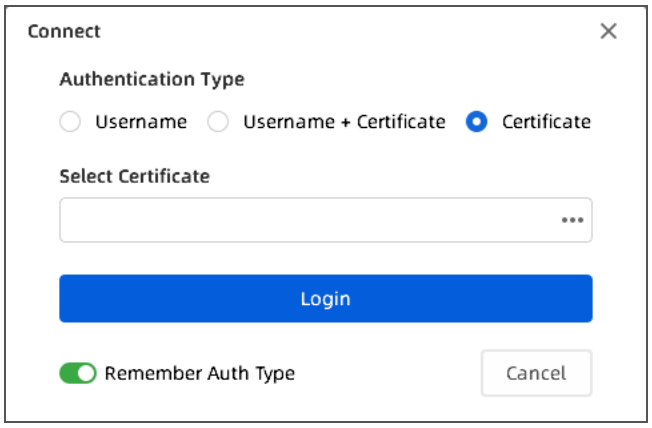
- If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local

AAA Server.

- After "OAuth2 authentication is successful" is displayed on the browser, you may not successfully log in to the SSL VPN/ZTNA client. There may be scenarios where the IP address is occupied. Please check the reason for failure on the client.
- If secondary authentication is enabled on the device and OAuth2 authentication is supported, secondary authentication will not be performed when the client uses the third-party application login for connection.
- When you select the third-party application login, if you do not perform authentication operation after the browser pops up, the client will prompt authentication timeout after 10 minutes.
- To roll back the client to an earlier version, you need to uninstall the current version before installing the earlier version. You cannot directly overwrite the existing version. Otherwise, an error about the connection configuration will appear and the connection will fail.
- When the client automatically reconnects, you need to perform OAuth2 authentication again.
- When you connect to the device (R10F4 and later F versions, R11 and later versions) that supports OAuth2 authentication, the client page returns the authentication type configured on the device. For example, if the device is configured with username/password and OAuth2 authentication, the **Connect** page on the

client displays the "Username/Password" and "Third Login" authentication types.

- When you connect to the device (version that is earlier than R10F4) that does not support the OAuth2 authentication, the **Connect** page on the client displays three authentication types by default. For example, if the device is configured with the certificate authentication only, you need to select Certificate on the Connect page so that the connection can be successful, as shown below:



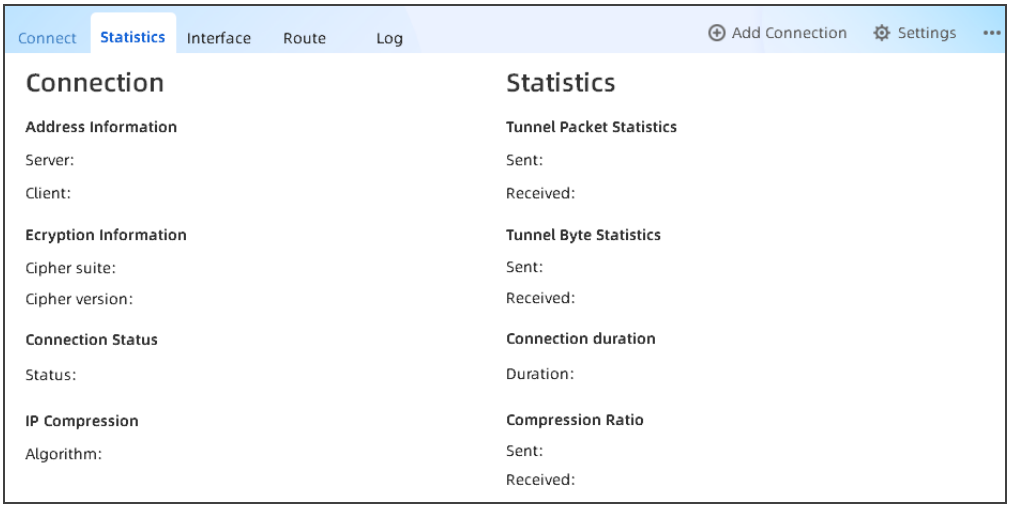
Finishing the above steps, the client will connect to the server automatically. After the connection has been established successfully, the icon ( ) will be displayed in the notification area. And the encrypted communication between the client and server can be implemented now.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the icon to edit the entry; and the icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.

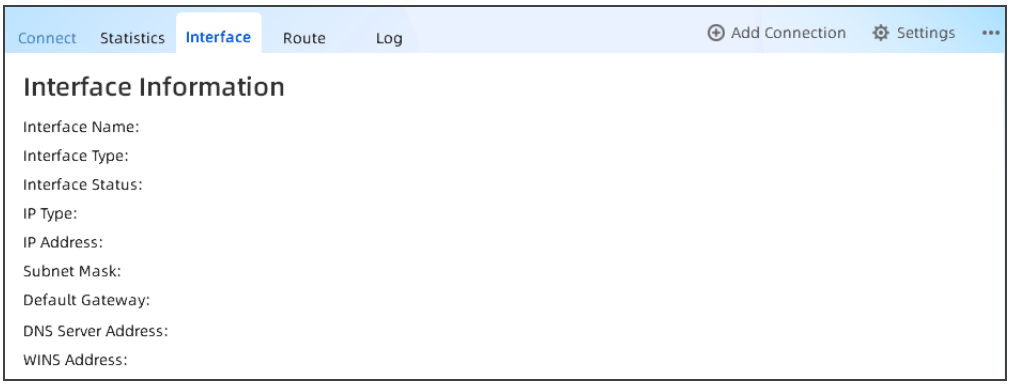


Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption Information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packet Statistics	
Send	The number of sent packets through the encryption tunnel.

Address Information: Shows the IP addresses	
Received	The number of received packets through the encryption tunnel.
Tunnel Byte Statistics	
Send	Bytes sent through the tunnel.
Received	Bytes received through the tunnel.
Connection duration	
Duration	Time period during which the client is online.
Compression Ratio	
Send	Length ratio of sent data after compression.
Received	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** tab to view routing information.

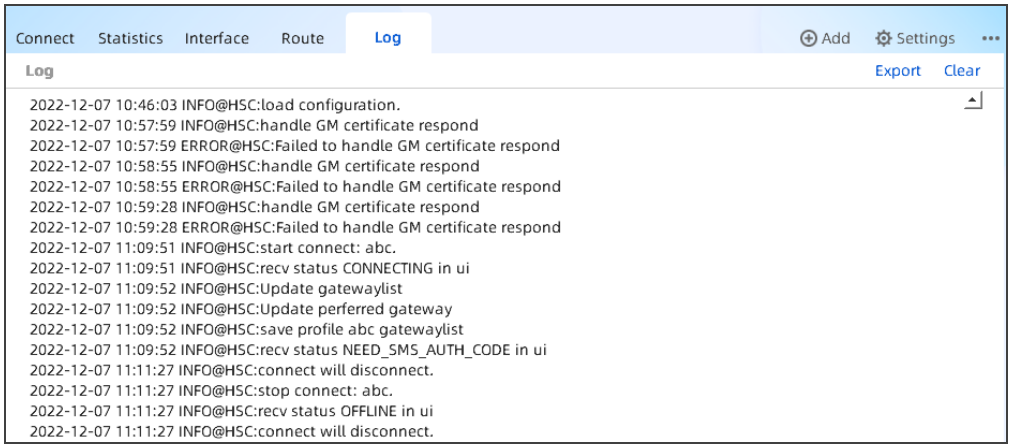


Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.

Option	Description
Interface Status	The status of the interface used to send encrypted data.
IP Type	The IP address type of the interface used to send encrypted data.
IP Address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet Mask	The subnet mask of the interface used to send encrypted data.
Default Gate-way	The default gateway address of the interface used to send encrypted data.
DNS Server Address	The address of the DNS server used by the client.
WINS Address	The address of the WINS server used by the client.

Viewing Log Information

On the client main page, click the **Log** tab to view log information.



Click ••• and select "Log Level" to set the level of logs to be displayed.

Configuring Check for Updates

On the client page, click and select **Check for Updates**. When an update is available, you can perform the following operations:

- Select **Update Immediately** to download the client immediately. After the client is downloaded, you are automatically redirected to the client installation page.
- Select **Update on Next Startup** to download the installation page to your PC, which will be installed on the next startup.
- Select **Do Not Remind Me Again**. When you start the client next time, the auto update prompt will no longer appear.

Third-party USB Key

Hillstone UKey certificate is the default certificate for the USB Key authentication. When authenticating with Hillstone UKey certificate, the client will select the Hillstone UKey certificate automatically and send it to the server, and the server will perform the authentication with the default certificate. This authentication process is transparent to the authenticated clients, i.e., the client need not to choose the certificate. If the third-party USB Key is used, you can set the third-party certificate as the default certificate to simplify the authentication process by using the tool named SelectUSBKey.

To set the third-party certificate to the default certificate, first you have to export the CSP Name of the USB Key in form of a registry file, and then add the exported file content to the registry of the client PC.

To export the CSP Name of the USB Key, take the following steps:

1. Install the driver of the third-party USB Key.
2. Insert the third-party USB Key.

3. Double click SelectUSBKey.exe, and the Select Default Certificate dialog is shown as below:

   Export: Exports the CSP Name of the USB Key in form of a registry file.

   Update: Refreshes the certificate list.

   Close: Closes the dialog.

4. Select the certificate you want from the certificate list, and then click **Export**.

After exporting the CSP Name of the USB Key, double click the exported file, and then add the content to the registry of the client PC. When authenticating with the third-party certificate, the client will automatically select the third-party USB Key certificate and send it to the server.

Client Menu

Right-click the green icon of the client, the client menu appears. Descriptions of the menu items:

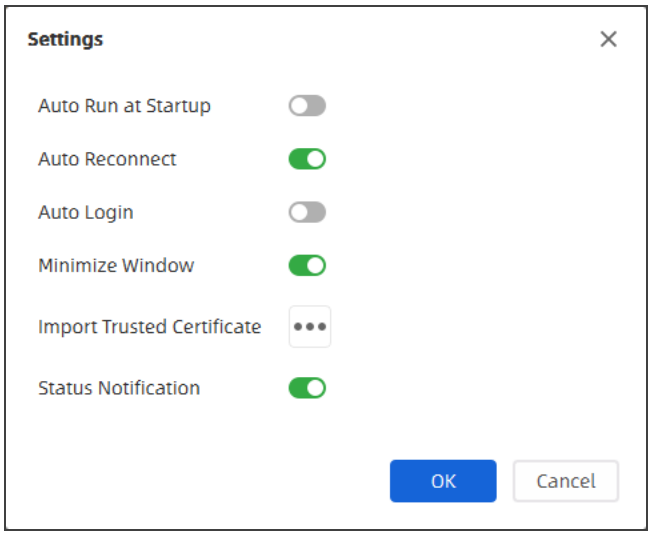
- **Change Password**: Displays the dialog for changing password.
- **Redirect URL**: When the device end has a redirect URL configured, users can click this menu to quickly jump to this URL address.
- **Resource List**: When accessing the SSL VPN service, user can click this menu to open the browser page displaying internal resources.
- **Application Resource List**: When a user successfully connects to a ZTNA service using the Secure Connect client, this menu is displayed. After the user logs in, a ZTNA portal page will be displayed. The user can click this menu to display the latest ZTNA portal page to view the application resource access privilege after it is closed. The portal page displays the application resources that the user is granted access and is not granted access. For those that the user is not granted access, the user can attempt to acquire the access privilege by adjusting the access terminal configurations. The application resources that the user is denied from accessing will not be displayed on the portal page. If a user is denied from accessing any application

resources, the portal page displays a message indicating that no Web resources are available to the user.

- **Show Window**: When Secure Connect client window is minimized, click this menu item to display the client main page.
- **Quit**: Click **Quit** to close the client.

General Configuration

Click **Settings** on the client main page.



- **Startup and automatic run**: Enable this option to automatically run the client when the PC is starting.
- **Automatic reconnect**: Enable this option to automatically reconnect to the SSL VPN/ZTNA server when the connection is hung up.
- **Automatic login**: Enable this option to allow the user to login using the connection information from the previous successful login automatically when the client is starting.
- **Minimize window**: Enable this option to allow the client window to be minimized.

- **Import trusted certificate**: After the Verify Server Cert function is enabled when establishing a connection, click button, and click **Import** on the<Trusted certificate>page to import the authentication certificate for the server. Click **Delete** to delete the trusted certificate in the list.
- **Status notification**: When the client connection is successful or failed, the corresponding status window appears.

Uninstalling the Client

To uninstall the client on your PC, from the Start menu, click **All Programs > Hillstone Secure Connect > Uninstall**.

Hillstone Secure Connect Client for Android

The SSL VPN/ZTNA client for Android is Hillstone Secure Connect. It can run in Android 8.x/Android 9.x/Android 10.x/Android 11.x/Android 12.x/Android 13.x/HongmengOS 2.0. The functions of Secure Connect Android client contain the following items:

- Obtain the interface information of the Android OS.
- Display the connection status with the device, traffic statistics, interface information, and routing information.
- Display the log information of the application.
- Collect and report endpoint status information.

Downloading and Installing the Client

To download and install the Secure Connect Android client, take the following steps:

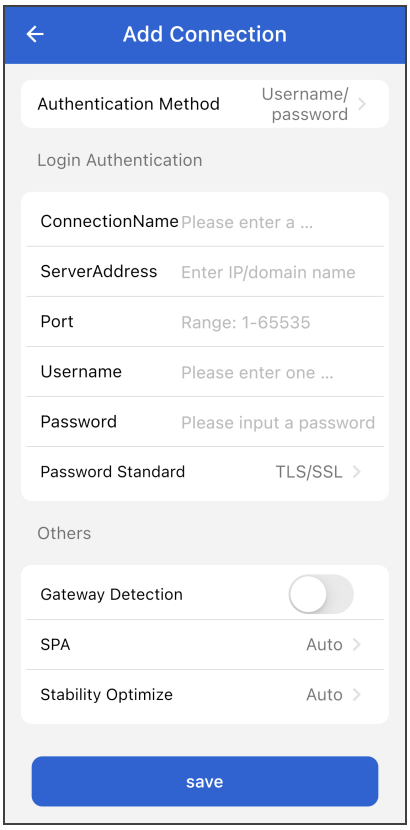
1. Visit https://www.hillstonenet.com/more/services/product-downloads/ to download the installation file of the client, or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. Use the Android device to scan the QR code of the Secure Connect Android client.
3. Open the URL and download the Hillstone-Secure-Connect-Versione_Number.apk file.
4. After downloading successfully, find this file in the Android device.
5. Click it and the installation starts.
6. Read the permission requirement.
7. Click **Install**.

Starting Up and Connecting

After the Secure Connect Windows client is installed successfully, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on the desktop and enter the client main page.

2. In the "Home" tab, click "+" and enter the "Add Connection" page.



Enter the connection information.

Option	Description
Authentication Method	Select the authentication method. "User name/password", "User name/password + Digital Certificate" and "Digital Certificate" are supported.
Connection Name	Enter the connection name.
Server Address	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Username	Enter the name of the login user. When authentication method

Option	Description
	is specified as "User name/password" or "User name/-password + Digital Certificate", the client user name and password should be entered.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
PIN	Enter the PIN code of the USB Key when the authentication type is "User name/password + Digital certificate" or "Digital certificate".
Password Standard	Select the SSL protocol type: • TLS/SSL: indicates the TLS/SSL protocol. • GMSSL: indicates the GUOMI SSL protocol.
Select Certificate	Select the digital certificate that has been imported into the Android device in advance.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs,

Option	Description
	the ZTNA client will switch to connect the gateway with the best link quality.
Optimal Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
Single Packet Authentication	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • On: When SPA is enabled, the knock port should be manually specified. By default, SPA is enabled. • Off: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA

Option	Description
	device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.



Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Select it and click **Connection Status** to start the connection.
5. If SMS authentication, token authentication or email authentication is enabled, you need to enter the corresponding authentication code to complete the authentication.

After the client connects to the SSL VPN/ZTNA server, the encrypted communication between the client and server can be implemented now.

Editing and Deleting Login Entry

To edit a login entry, click the  icon;

To delete a login entry, press it and drag it to the right.

Viewing Connection Information

Click "Information" tab on the client main page to view connection statistics, interface and routing information.

Option	Description
Server Address	IP address of the connected SSL VPN/ZTNA server.
Port	Port number of the connected SSL VPN/ZTNA server.
User Name	Login user name of the connected SSL VPN/ZTNA server.
Connection Duration	Time period during which the client is online.
Receive Bytes	Received bytes through the encryption tunnel.
Send Bytes	Sent bytes through the encryption tunnel.
Receive Packets	Number of received packets through the encryption tunnel.
Send Packets	Number of sent packets through the encryption tunnel.
Receive Compression Rate	Length ratio of received data after compression.
Send Compression Rate	Length ratio of sent data after compression.

Interface statistics:

Option	Description
Interface Name	The name of the interface used to send encrypted data.

Option	Description
Interface Type	The type of the interface used to send encrypted data.
Interface State	The status of the interface used to send encrypted data.
Physical Address	The MAC address of the interface used to send encrypted data.
IP Address Type	The IP address type of the interface used to send encrypted data.
Network Address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet Mask	The subnet mask of the interface used to send encrypted data.
Default Gate-way	The default gateway address of the interface used to send encrypted data.
DNS Address	The address of the DNS server used by the client.

Hillstone Secure Connect Client for iOS

The SSL VPN/ZTNA client for iOS is Hillstone Secure Client. It supports iOS 12.x/iOS 13.x/iOS 14.x/iOS 15.x/iOS 16.x versions. The Secure Connect iOS client mainly has the following functions:

- Simplify the tunnel creation process between the iOS device and the Hillstone device
- Display the connection status between the iOS device and the Hillstone device
- Display the log information
- Collect and report endpoint device status information.

Downloading and Installing the Client

You can take either of the following methods to download and install the Secure Connect iOS client:

- Search Hillstone Secure Client(beta) in the App Store.
- Visit https://www.hillstonenet.com/more/services/product-downloads/, locate the QR code for iOS client, use the iOS device to scan the code and then jump to App Store for downloading and installation.
- Visit https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance

Starting Up and Connecting

After the client is installed successfully, for the first time login, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on the desktop and enter the client main page.
2. In the "Home" tab, click "+" and enter the "Add Connection" page.

   Enter the connection information.

Option	Description
Connection Name	Enter the connection name.
Server Address	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
User name	Enter the name of the login user

Option	Description
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Password Standard	Select the SSL protocol type: • TLS/SSL: indicates the TLS/SSL protocol. • GMSSL: indicates the GUOMI SSL protocol.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality.
Optimal Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.

Option	Description
Single Packet Authentication	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • On: When SPA is enabled, the knock port should be manually specified. By default, SPA is enabled. • Off: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.

Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Select it and click **Connection Status** to start the connection.
5. If SMS, token or email authentication is enabled, type the corresponding code to complete the authentication.
6. After login, the iOS device will start the VPN configuration deployment automatically. In the **Would Like to Add VPN Configurations** page, click **Allow**.
7. Enter your passcode. The passcode is the one for unlocking your iOS screen. With the correct passcode entered, the iOS device starts to install the profile.
8. After the installation is complete, start **Settings** of the iOS device and navigate to **VPN**.
9. Select the configured connection name and click the **Connect** button.
10. After the client connects to the SSL VPN/ZTNA server, the encrypted communication between the client and server can be implemented now.

Notes: For subsequent logins, you do not need to perform the VPN configuration deployment steps. You can log in the client and start the connection directly.

Editing and Deleting Login Entry

To edit a login entry, click the icon;

To delete a login entry, press it and drag it to the right.

Viewing Connection Information

Click "Information" tab on the client main page to view connection statistics, interface and routing information.

Option	Description
Server Address	IP address of the connected SSL VPN/ZTNA server.
Port	Port number of the connected SSL VPN/ZTNA server.
User Name	Login user name of the connected SSL VPN/ZTNA server.
Connection Duration	Time period during which the client is online.
Receive Bytes	Received bytes through the encryption tunnel.
Send Bytes	Sent bytes through the encryption tunnel.
Receive Packets	Number of received packets through the encryption tunnel.
Send Packets	Number of sent packets through the encryption tunnel.
Receive Compression Rate	Length ratio of received data after compression.
Send Compression Rate	Length ratio of sent data after compression.

Interface statistics:

Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface State	The status of the interface used to send encrypted data.
Physical Address	The MAC address of the interface used to send encrypted data.
IP Address Type	The IP address type of the interface used to send encrypted data.
Network Address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet Mask	The subnet mask of the interface used to send encrypted data.
Default Gate-way	The default gateway address of the interface used to send encrypted data.
DNS Address	The address of the DNS server used by the client.

Hillstone Secure Connect Client for macOS

The SSL VPN/ZTNA client for macOS is Hillstone Secure Connect. It can run in macOS 10.13/macOS 10.14/macOS 10.15/macOS 11.0/macOS 12.0/macOS 13.0 versions. The encrypted data can be transmitted between the client and the SSL VPN/ZTNA server after a connection has been established successfully. The functions of the client are:

- Establish the encrypted connection with the SSL VPN/ZTNA server.
- Show the connection status, traffic statistics, and route information.

- Show log messages.
- Collect and report endpoint device status information.

Downloading and Installing the Client

To download and install the Secure Connect macOS client, take the following steps:

1. Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/ or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. After downloading the installation file, double-click it. In the pop-up, drag the Secure Connect macOS client to the **Applications** folder to perform the installation.



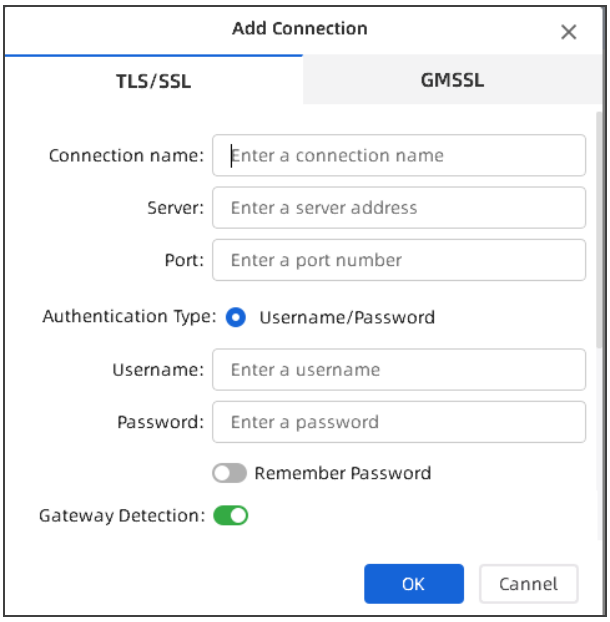
Notes: To open the installation file, you must have the administrator permission and select **Anywhere in System Preferences > Security & Privacy > General > Allow apps downloaded from**.

Starting Up and Connecting

After the Secure Connect macOS client is installed successfully, take the following steps to start and log in the client:

1. Select **Launchpad > Hillstone Secure Connect**. The client starts.

2. Click **Add**. The following dialog box is displayed.



Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
GMSSL	Select this tab to use the GMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Authentication Type	The authentication type is username/password.
Username	Enter the name of the login user.
Password	Enter the password of the login user. If local authentication

Option	Description
	server is configured on the device, the user name and password should be configured in advance on the device.
Remember Password	After this option is selected, you do not need to enter the user's password at the next-time connection.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port

Option	Description
	number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.
Verify Server Cert	Click **Enable** button to verify the certificate of the server when establishing the connection. To add trusted certificates, please refer to General Configuration.

> **Tips:** If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous step to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. The client will attempt to establish a connection to the device.
5. If SMS authentication, email authentication or token authentication is enabled, enter the corresponding authentication code to complete the authentication.

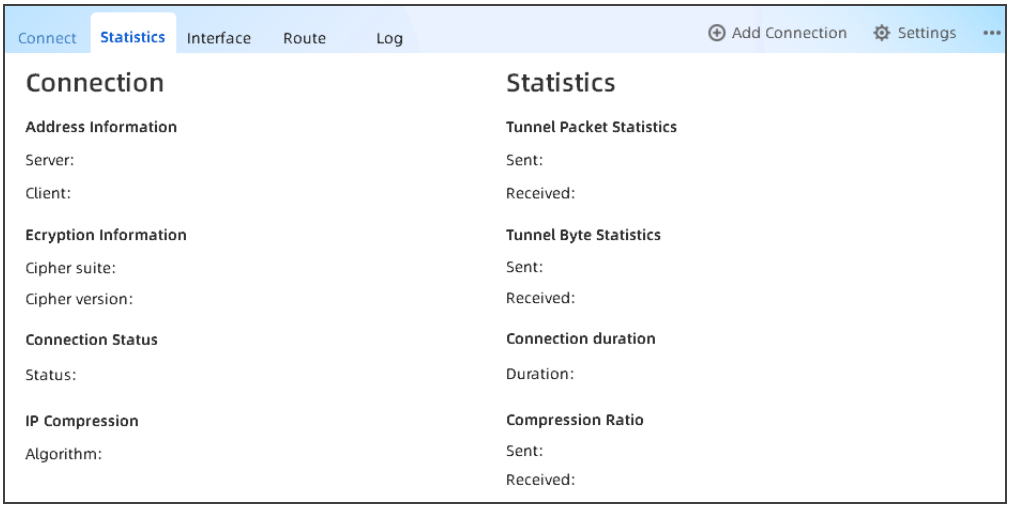
Finishing the above steps, the client will connect to the server automatically.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the  icon to edit the entry; and the  icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.

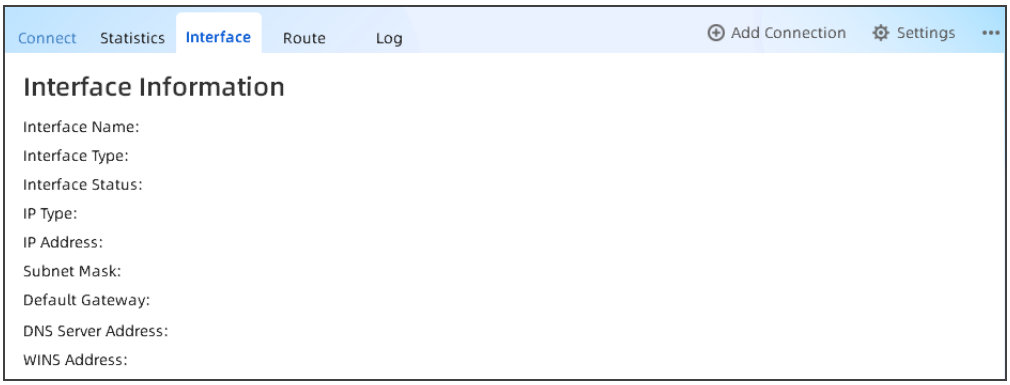


Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption Information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packets	
Send	The number of sent packets through the encryption tunnel.

Address Information: Shows the IP addresses	
Received	The number of received packets through the encryption tunnel.
Tunnel Bytes	
Send	Bytes sent through the tunnel.
Received	Bytes received through the tunnel.
Connection duration	
Duration	Time period during which the client is online.
Compression Ratio	
Send	Length ratio of sent data after compression.
Received	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** tab to view routing information.

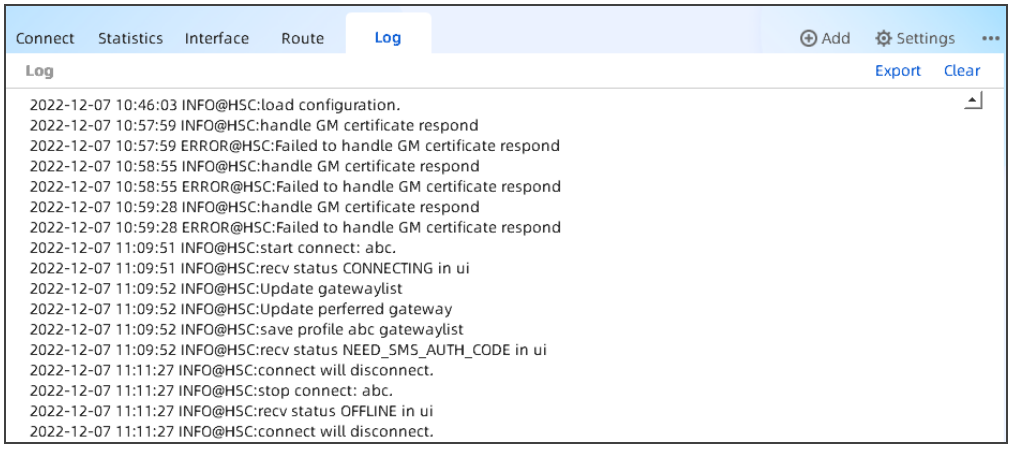


Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface Status	The status of the interface used to send encrypted data.

Option	Description
IP Type	The IP address type of the interface used to send encrypted data.
IP Address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet Mask	The subnet mask of the interface used to send encrypted data.
Default Gate-way	The default gateway address of the interface used to send encrypted data.
DNS Server Address	The address of the DNS server used by the client.
WINS Address	The address of the WINS server used by the client.

Viewing Log Information

On the client main page, click the **Log** tab to view log information.



Click ••• and select "Log Level" to set the level of logs to be displayed.

Configuring Check for Updates

On the client page, click and select **Check for Updates**. When an update is available, you can perform the following operations:

- Select **Update Immediately** to download the client immediately. After the client is downloaded, you are automatically redirected to the client installation page.
- Select **Update on Next Startup** to download the installation page to your PC, which will be installed on the next startup.
- Select **Do Not Remind Me Again**. When you start the client next time, the auto update prompt will no longer appear.

Client Menu

Right-click the green icon of the client, the client menu appears. Descriptions of the menu items:

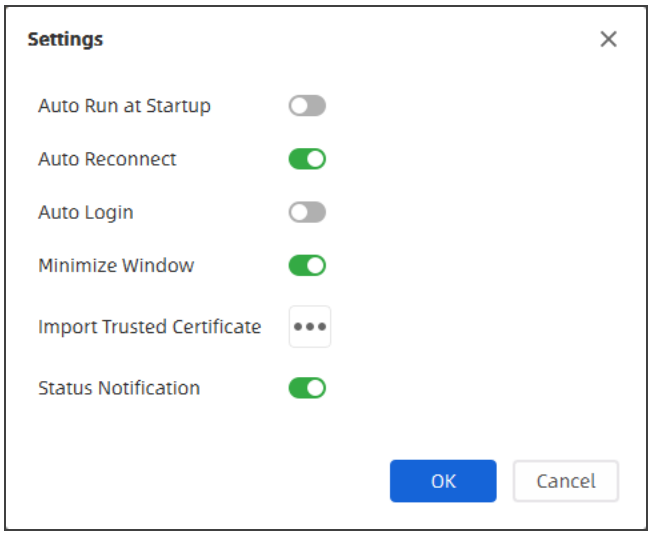
- **Redirect URL**: When the device end has a redirect URL configured, users can click this menu to quickly jump to this URL address.
- **Resource List**: When accessing the SSL VPN service, user can click this menu to open the browser page displaying internal resources.
- **Application Resource List**: When a user successfully connects to a ZTNA service using the Secure Connect client, this menu is displayed. After the user logs in, a ZTNA portal page will be displayed. The user can click this menu to display the latest ZTNA portal page to view the application resource access privilege after it is closed. The portal page displays the application resources that the user is granted access and is not granted access. For those that the user is not granted access, the user can attempt to acquire the access privilege by adjusting the access terminal configurations. The application resources that the user is denied from accessing will not be displayed on the portal page. If a user is denied from accessing any application

resources, the portal page displays a message indicating that no Web resources are available to the user.

- **Show Window**: When Secure Connect client window is minimized, click this menu item to display the client main page.
- **Quit**: Click **Quit** to close the client.

General Configuration

Click **Settings** on the client main page.



- **Automatic reconnect**: Enable this option to automatically reconnect to the SSL VPN/ZTNA server when the connection is hung up.
- **Automatic login**: Enable this option to allow the user to login using the connection information from the previous successful login automatically when the client is starting.
- **Minimize window**: Enable this option to allow the client window to be minimized.
- **Import trusted certificate**: After the Verify Server Cert function is enabled when establishing a connection, click ••• button, and click **Import** on the<Trusted certificate>page to import

the authentication certificate for the server. Click **Delete** to delete the trusted certificate in the list.

- **Status notification**: When the client connection is successful or failed, the corresponding status window appears.

Uninstalling the Client

To uninstall the client, right-click the client icon and select Move to Trash from the drop-down-list.

Hillstone Secure Connect Client for Linux

The SSL VPN/ZTNA client for Linux is Hillstone Secure Connect. It can run in the following operation systems:

- CentOS 7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.3/8.4/8.5
- Ubuntu 18.04/18.10/19.04/19.10/20.04/20.10/21.04
- Ubuntu Kylin 18.04/20.04

The encrypted data can be transmitted between the client and the SSL VPN/ZTNA server after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC in which the client is running.
- Show the connection status, traffic statistics, and route information.
- Show log messages.
- Collect and report endpoint status information.

Take CentOS 7.6 as an example to introduce downloading and installing client, starting client and establishing connection, upgrading and uninstalling client, the client GUI and menu. The client configuration of other three Linux systems can refer to 64-bit Ubuntu Kylin16.04 desktop.

Downloading and Installing the Client

To download and install the Secure Connect Linux client, take the following steps:

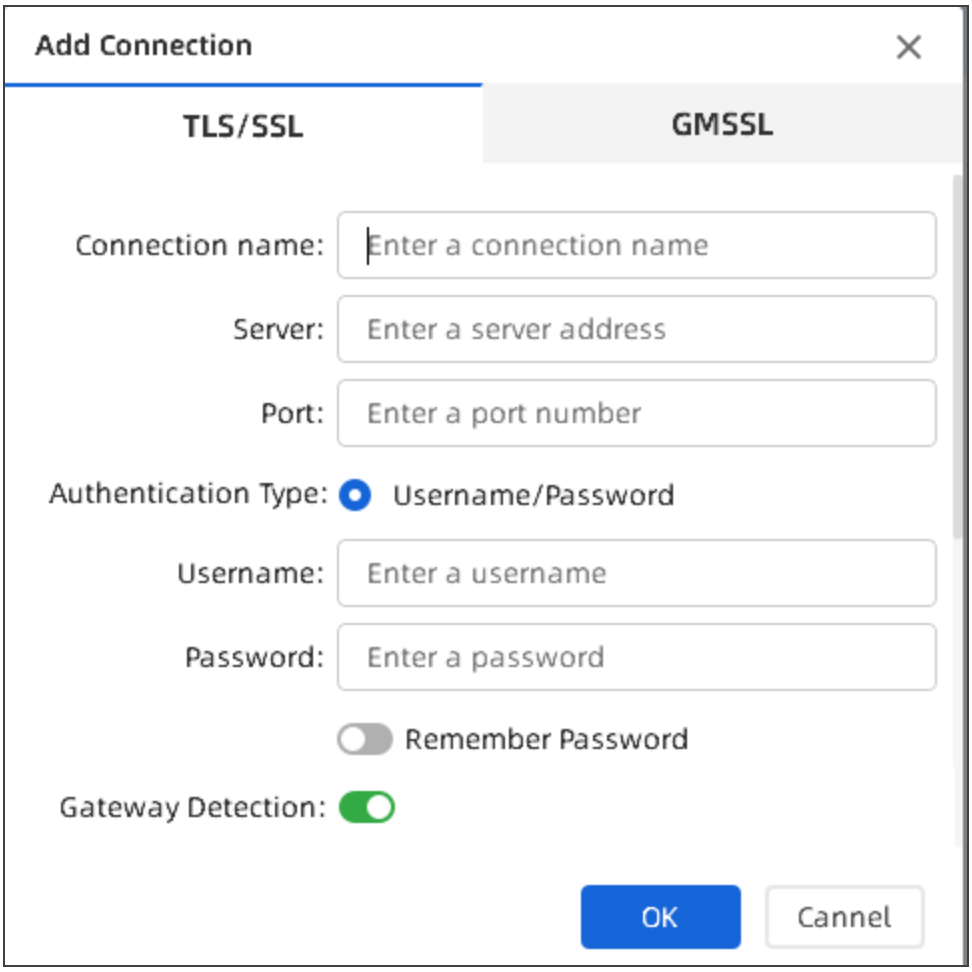
1. Visit Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/, or https://IP-Address:Port-Number on the device side. In the URL, IP-Address and Port-Number refer to the IP address and HTTPS port number of the egress interface specified in the SSL VPN/ZTNA instance.
2. After downloading the installation file, right-click the client icon and select **Properties** to go to the properties page. In the properties page, click **Permissions** tab and check **Allow executing files as program**, then close it.
3. Double-click the client icon and follow the setup wizard to complete the installation.

Starting Up and Connecting

After the Secure Connect Linux client is installed successfully, take the following steps to start and log in the client:

1. Double-click the Hillstone Secure Connect icon on your desktop. The client main page is displayed.

2. Click **Add**. The following dialog box is displayed.



Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
GMSSL	Select this tab to use the GMSSL protocol.
Connection Name	Enter the connection name.
Server	Enter the IP address of SSL VPN or ZTNA server.

Option	Description
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
User name	Enter the name of the login user.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password should be configured in advance on the device.
Remember Password	After this option is enabled, you do not need to enter the user's password at the next-time connection.
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect

Option	Description
	the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.
Verify Server Cert	Click **Enable** button to verify the certificate of the server when establishing the connection. To add trusted certificates, please

Option	Description
	refer to General Configuration.

Tips: If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.
4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. The client will attempt to establish a connection to the device.
5. If SMS authentication, email authentication or token authentication is enabled, enter the corresponding authentication code to complete the authentication.

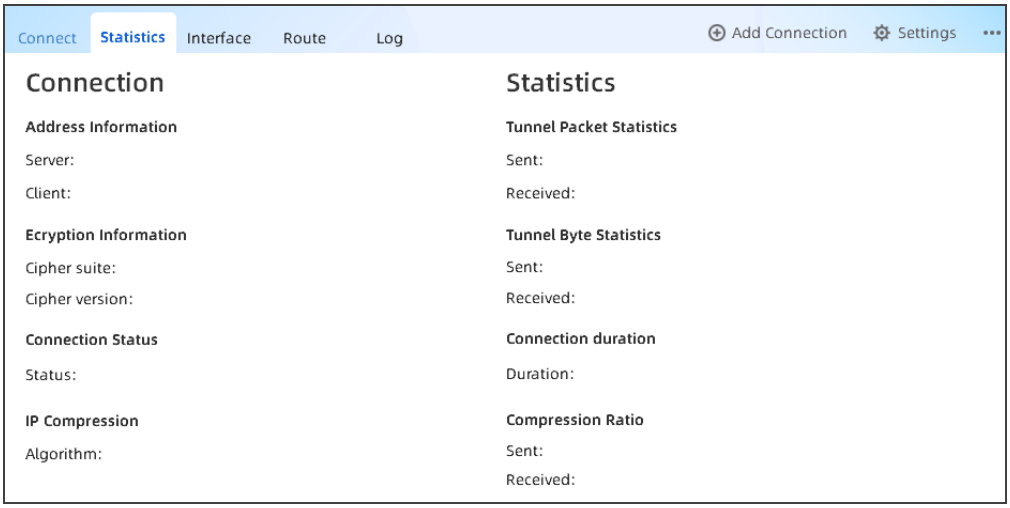
After the client connects to the SSL VPN/ZTNA server, the encrypted data can be transmitted between the client and the server now.

Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the  icon to edit the entry; and the  icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.

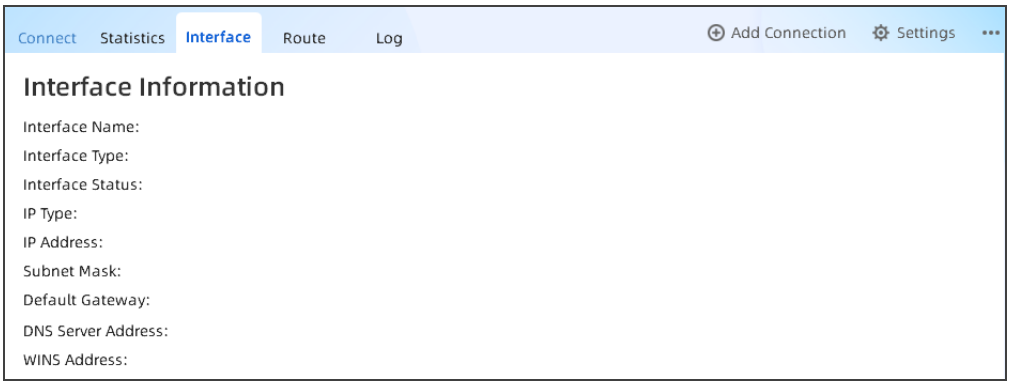


Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption Information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.
IP Compression	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packet Statistics	
Send	The number of sent packets through the encryption tunnel.

Address Information: Shows the IP addresses	
Received	The number of received packets through the encryption tunnel.
Tunnel Byte Statistics	
Send	Bytes sent through the tunnel.
Received	Bytes received through the tunnel.
Connection duration	
Duration	Time period during which the client is online.
Compression Ratio	
Send	Length ratio of sent data after compression.
Receive	Length ratio of received data after compression.

Viewing Interface and Routing Information

On the client main page, click the **Interface** tab to view interface information; click the **Route** tab to view routing information.

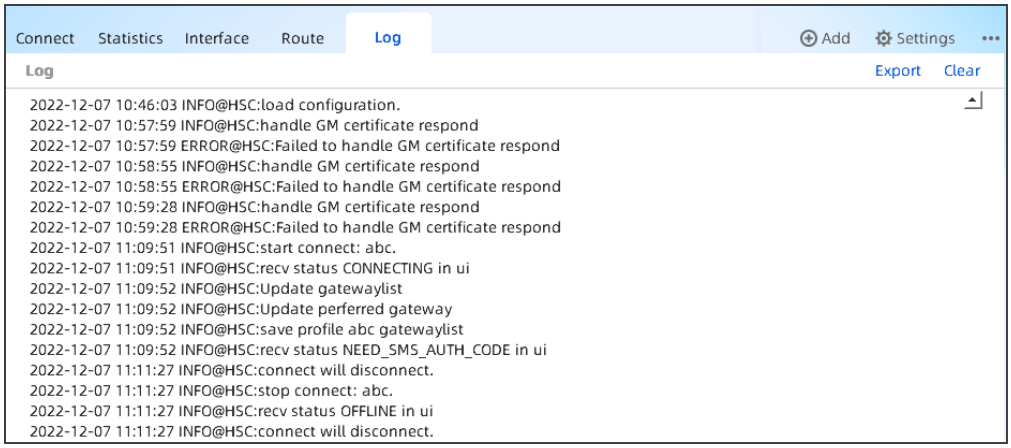


Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.

Option	Description
Interface Status	The status of the interface used to send encrypted data.
IP Type	The IP address type of the interface used to send encrypted data.
IP Address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet Mask	The subnet mask of the interface used to send encrypted data.
Default Gate-way	The default gateway address of the interface used to send encrypted data.
DNS Server Address	The address of the DNS server used by the client.
WINS Address	The address of the WINS server used by the client.

Viewing Log Information

On the client main page, click the **Log** tab to view log information.



Click ••• and select "Log Level" to set the level of logs to be displayed.

Configuring Check for Updates

On the client page, click and select **Check for Updates**. When an update is available, you can perform the following operations:

- Select **Update Immediately** to download the client immediately. After the client is downloaded, you are automatically redirected to the client installation page.
- Select **Update on Next Startup** to download the installation page to your PC, which will be installed on the next startup.
- Select **Do Not Remind Me Again**. When you start the client next time, the auto update prompt will no longer appear.

Client Menu

Right-click the green icon of the client, the client menu appears. Descriptions of the menu items:

- **Change Password**: Displays the dialog for changing password.
- **Redirect URL**: When the device end has a redirect URL configured, users can click this menu to quickly jump to this URL address.
- **Resource List**: When accessing the SSL VPN service, user can click this menu to open the browser page displaying internal resources.
- **Application Resource List**: When a user successfully connects to a ZTNA service using the Secure Connect client, this menu is displayed. After the user logs in, a ZTNA portal page will be displayed. The user can click this menu to display the latest ZTNA portal page to view the application resource access privilege after it is closed. The portal page displays the application resources that the user is granted access and is not granted access. For those that the user is not granted access, the user can attempt to acquire the access privilege by adjusting the access

terminal configurations. The application resources that the user is denied from accessing will not be displayed on the portal page. If a user is denied from accessing any application resources, the portal page displays a message indicating that no Web resources are available to the user.

- **Show Window**: When Secure Connect client window is minimized, click this menu item to display the client main page.
- **Quit**: Click **Quit** to close the client.

General Configuration

Click **Settings** on the client main page.

- **Automatic reconnect**: Enable this option to automatically reconnect to the SSL VPN/ZTNA server when the connection is hung up.
- **Automatic login**: Enable this option to allow the user to login using the connection information from the previous successful login automatically when the client is starting.
- **Minimize window**: Enable this option to allow the client window to be minimized.
- **Import trusted certificate**: After the Verify Server Cert function is enabled when establishing a connection, click button, and click **Import** on the<Trusted certificate>page to import the authentication certificate for the server. Click **Delete** to delete the trusted certificate in the list.
- **Client certificate management**: Click . On the Client Certificate Management page, click **Import** to import the certificate for login authentication, which is in the PKCS#12 format. You can import GM certificate and non-GM certificate. At most 16 certificate files can be imported. To delete a certificate in the list, click **Delete**.

- **Status notification**: When the client connection is successful or failed, the corresponding status window appears.

Hillstone Secure Connect Client for ChineseOS

The SSL VPN/ZTNA client for ChineseOS is Hillstone Secure Connect. It can run in the following operation systems:

- UOS 20 (CPU HiSilicon Kirin)
- Kylin V10 (CPU Zhaoxin)
- UOS 20 (CPU Feiteng)

Hillstone Secure Connect Client for ChineseOS will be supported in Kylin V10 (CPU HiSilicon Kirin), Kylin V10 (CPU Loongson), Kylin V10 (CPU Feiteng), UOS 20 (CPU Loongson), and UOS 20 (CPU Zhaoxin) later.

The encrypted data can be transmitted between the client and the SSL VPN/ZTNA server after a connection has been established successfully. The functions of the client are:

- Get interface and route information from the PC in which the client is running.
- Show the connection status, traffic statistics, and route information.
- Show log messages.
- Collect and report endpoint status information.

This section mainly describes how to download, install, start, uninstall Secure Connect Client for ChineseOS, and gives instructions on how to use its GUI and menu. The device side supports the following authentication methods:

- Username/Password
- Username/Password + Certificate

- Certificate
- Third-party Application Login (OAuth2 Authentication)

Take UOS 20 as an example to introduce downloading and installing client, starting client and establishing connection, upgrading and uninstalling client, the client GUI and menu. The client configuration of other ChineseOS systems is similar.

Downloading and Installing the Client

To download and install the Secure Connect ChineseOS client, take the following steps:

1. Visit the APP Store that comes with ChineseOS and search for the Hillstone Secure Connect client.
2. Click **Install** to install the client. After the client is installed, the **Open** button is displayed. You can click **Open** to start up the client.

Starting Up and Connecting

After the Secure Connect ChineseOS client is installed successfully, take the following steps to start and log in the client:

1. In the **Start** menu, click **Hillstone Secure Connect**. You can also right-click **Hillstone Secure Connect** to add a shortcut or fix the client to taskbar.
2. Click **Add**.

   Enter the connection information.

Option	Description
TLS/SSL	Select this tab to use the TLS/SSL protocol.
GMSSL	Select this tab to use the GMSSL protocol.
Connection Name	Enter the connection name.

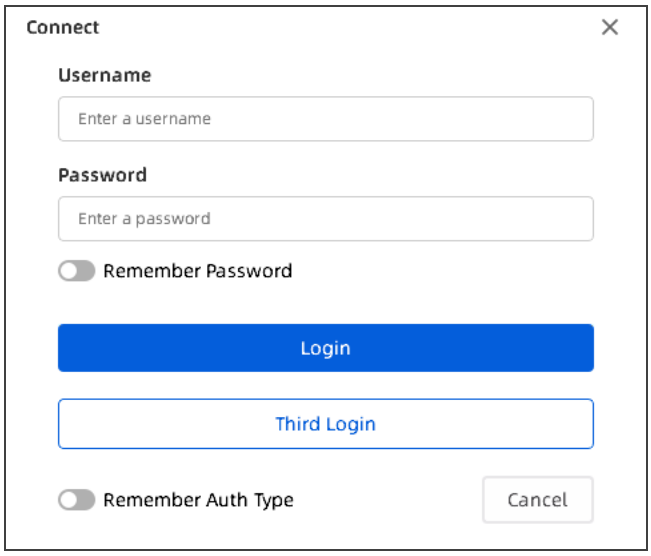
Option	Description
Server	Enter the IP address of SSL VPN or ZTNA server.
Port	Enter the HTTPS port number of SSL VPN or ZTNA server.
Advanced Config: By default, advanced configurations are hidden. You can click › to expand this section and configure the following options.	
Gateway Detection	Set whether to enable the gateway detection function, which applies in the ZTNA access scenario. If the ZTNA device has backup gateway configured, ZTNA users can enable gateway detection on ZTNA clients. When a user logs in, the ZTNA client will obtain the backup gateway list, detect the link quality of each gateway and establish a connection to the one with the best link quality. After the connection is established, the ZTNA client will detect and update the link quality of all gateways every 30 minutes. If a connection or login failure occurs, the ZTNA client will switch to connect the gateway with the best link quality. It is enabled by default.
Preferred Gateway	After gateway detection is enabled, the ZTNA client will obtain the backup gateway list during user login. At this time, users can manually select a preferred gateway. By default, the preferred gateway is not set. If it is set, the ZTNA client will preferentially connect it when the user logs in via this client again. If the connection fails, the ZTNA client will switch to connect the gateway with the best link quality.
SPA	Set whether to enable the SPA function, which applies in the ZTNA access scenario. If the ZTNA device has SPA enabled

Option	Description
	and is configured with hidden IP address and port number, ZTNA users also need to enable SPA on ZTNA clients. When a user logs in via the ZTNA client, the user needs to pass single packet authorization before establishing a connection to the ZTNA device. When SPA is disabled or is enabled but not configured with hidden IP address and port number on the ZTNA device, the ZTNA device will no perform single packet authorization on the clients no matter whether SPA is enabled on clients. • Enable: When SPA is enabled, the knock port should be manually specified. • Disable: When SPA is disabled, ZTNA clients will not knock when logging in. • Auto: No matter whether SPA is enabled on the ZTNA device, clients consider that the ZTNA device requires single packet authorization and knocks on the default knock port number. This is the default option.
Stability Optimization	Set whether to use TCP for data transmission. It is disabled by default. To use it, make sure the device side has the TCP port configured. It is disabled by default.
Verify Server Cert	Click **Enable** button to verify the certificate of the server when establishing the connection. To add trusted certificates, please refer to General Configuration.

3. After the connection information configuration is completed, click **OK**. The system will save a login entry. If needed, you can repeat the previous steps to add more login entries.

4. On the client main page, the configured connection information has been saved as a login entry. Click **Connect**. On the Connect dialog box, select an authentication type and log in. The client will attempt to establish a connection to the device.

   The authentication type includes username/password, username/password+certificate, certificate, and third-party application login. If the access user on the device selects an OAuth2 server, OAuth2 authentication will be used as the third-party application login. In this case, you will be redirected to the OAuth2 authentication process: click the OAuth2 authentication icon, enter the OAuth2 authentication page, the browser will return the authentication result after the OAuth2 authorization and authentication are completed, and a login status will be returned to the client.



Option	Description
Username	Enter the name of the login user. When Auth type is specified as "Username" or "Username + Certificate", the client user name and password should be entered.
Password	Enter the password of the login user. If local authentication server is configured on the device, the user name and password

Option	Description
	should be configured in advance on the device.
Certificate	When the authentication type is "Username + Certificate" or "Certificate", click this option to enter the dialog box for selecting a certificate. The selected certificate will be sent to the device for authentication.
Remember Password	After this option is selected, you do not need to enter the user's password at the next-time connection.
Remember Auth Type	after this option is selected, this authentication type will be directly used upon next connection. By default, this option is selected. If you disable this function, you need to select an authentication type again upon next connection. **Note**: When the authentication type on the device changes, if the remembered authentication type is not included in the changed authentication type, you will be prompted that the authentication type is different from that on the device upon your next connection. In this case, you need to select an authentication type again.

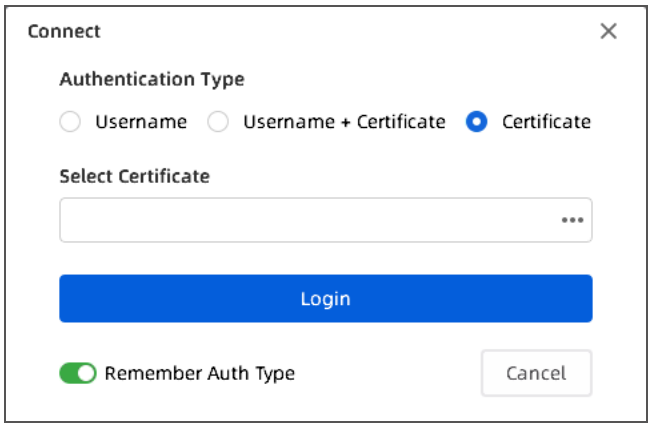
5. If SMS authentication, token authentication, or Email authentication is enabled, type the corresponding authentication code to pass the secondary authentication.

6. Finishing the above steps, the client will connect to the server automatically. After the connection has been established successfully, the encrypted communication between the client and server can be implemented now.

Tips:

- If the password control function and the change password function are enabled on the device, for example: the system will remind the user to change the password before and after the password expires, and verify the historical password to ensure that the new password is different from the previous password. For more information about password control function, refer to Configuring a Local AAA Server.
- After "OAuth2 authentication is successful" is displayed on the browser, you may not successfully log in to the SSL VPN/ZTNA client. There may be scenarios where the IP address is occupied. Please check the reason for failure on the client.
- If secondary authentication is enabled on the device and OAuth2 authentication is supported, secondary authentication will not be performed when the client uses the third-party application login for connection.
- When you select the third-party application login, if you do not perform authentication operation after the browser pops up, the client will prompt authentication timeout after 10 minutes.
- To roll back the client to an earlier version, you need to uninstall the current version before installing the earlier version. You cannot directly overwrite the existing version. Otherwise, an error about the connection configuration will appear and the connection will fail.

- When the client automatically reconnects, you need to perform OAuth2 authentication again.
- When the client is connected to the device (R10F4 and later F versions, R11 and later versions) that supports OAuth2 authentication, the client page returns the authentication type configured on the device. For example, if the device is configured with username/password and OAuth2 authentication, the **Connect** page on the client displays the "Username/Password" and "Third Login" authentication types.
- When the client is connected to the device (version that is earlier than R10F4) that does not support the OAuth2 authentication, the **Connect** page on the client displays three authentication types by default. For example, if the device is configured with the certificate authentication only, you need to select Certificate on the Connect page so that the connection can be successful, as shown below:

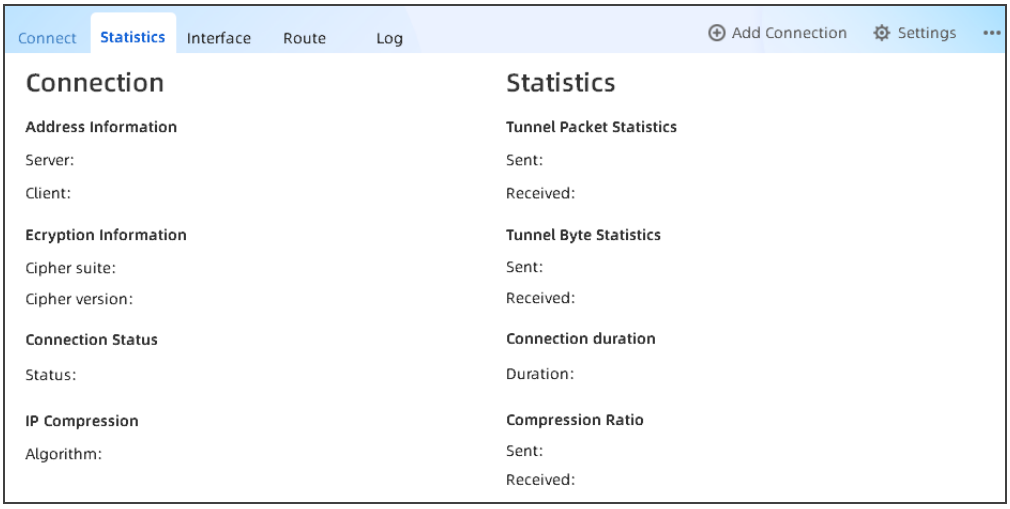


Editing and Deleting Login Entry

To edit or delete a login entry, place the cursor on the login entry. Click the icon to edit the entry; and the icon to delete the entry.

Viewing Connection and Statistics Information

On the client main page, click the **Statistics** tab to view connection and statistics information.

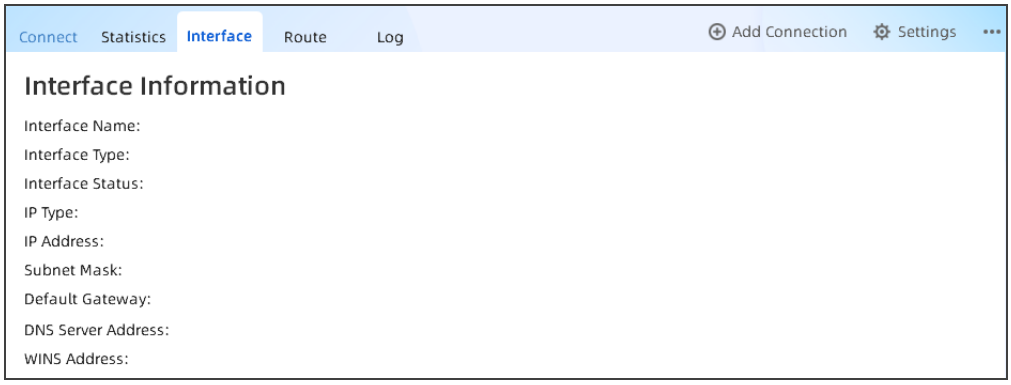


Address Information: Shows the IP addresses	
Server	The IP address of the connected SSL VPN/ZTNA server.
Client	The IP address of the client.
Encryption Information: Shows the encryption information.	
Cipher suite	The encryption algorithm and authentication algorithm used by SSL VPN/ZTNA.
Cipher version	The SSL version used by SSL VPN/ZTNA.
Connection Status	
Status	The current connecting state between the client and server.

Address Information: Shows the IP addresses	
IP Compress	
Algorithm	Shows the compression algorithm used by SSL VPN/ZTNA.
Tunnel Packet Statistics	
Send	The number of sent packets through the encryption tunnel.
Received	The number of received packets through the encryption tunnel.
Tunnel Byte Statistics	
Send	Bytes sent through the tunnel.
Received	Bytes received through the tunnel.
Connection duration	
Duration	Time period during which the client is online.
Compression Ratio	
Send	Length ratio of sent data after compression.
Received	Length ratio of received data after compression.

Viewing Interface and Routing Information

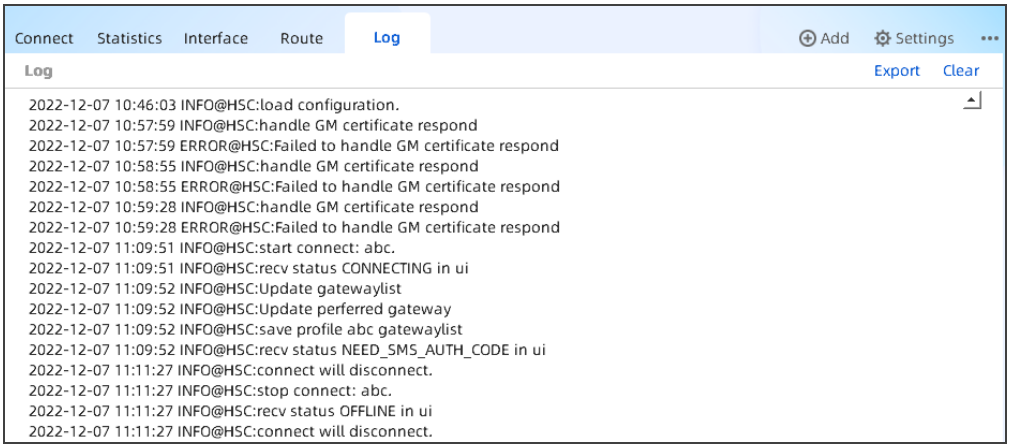
On the client main page, click the **Interface** tab to view interface information; click the **Route** tab to view routing information.



Option	Description
Interface Name	The name of the interface used to send encrypted data.
Interface Type	The type of the interface used to send encrypted data.
Interface Status	The status of the interface used to send encrypted data.
IP Type	The IP address type of the interface used to send encrypted data.
IP Address	The IP address (allocated by the device) of the interface used to send encrypted data.
Subnet Mask	The subnet mask of the interface used to send encrypted data.
Default Gate-way	The default gateway address of the interface used to send encrypted data.
DNS Server Address	The address of the DNS server used by the client.
WINS Address	The address of the WINS server used by the client.

Viewing Log Information

On the client main page, click the **Log** tab to view log information.



Click ••• and select "Log Level" to set the level of logs to be displayed.

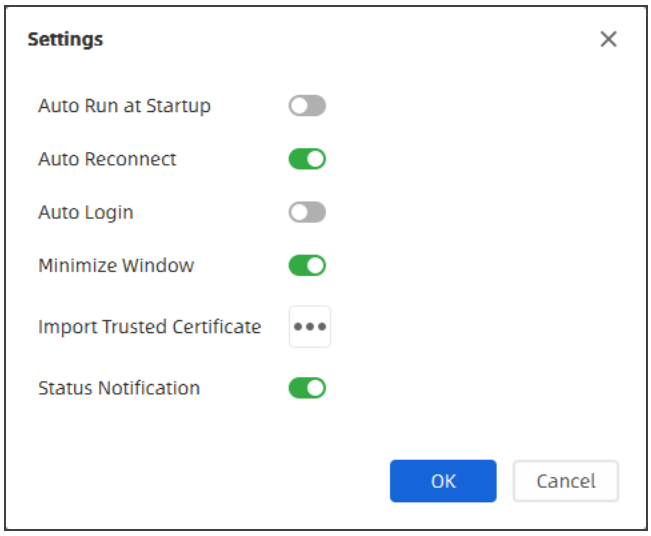
Configuring Check for Updates

On the client page, click ••• and select **Check for Updates**. When an update is available, you can perform the following operations:

- Select **OK** to download and install the latest client from the APP store that comes with ChineseOS.
- Select **Do Not Remind Me Again**. When you start the client next time, the auto update prompt will no longer appear.

General Configuration

Click **Settings** on the client main page.



- **Automatic reconnect**: Enable this option to automatically reconnect to the SSL VPN/ZTNA server when the connection is hung up.
- **Automatic login**: Enable this option to allow the user to login using the connection information from the previous successful login automatically when the client is starting.
- **Minimize window**: Enable this option to allow the client window to be minimized.

- **Import trusted certificate**: After the Verify Server Cert function is enabled when establishing a connection, click  button, and click **Import** on the<Trusted certificate>page to import the authentication certificate for the server. Click **Delete** to delete the trusted certificate in the list.
- **Status notification**: When the client connection is successful or failed, the corresponding status window appears.

General Configuration

Click **Settings** on the client main page.

- **Automatic reconnect**: Enable this option to automatically reconnect to the SSL VPN/ZTNA server when the connection is hung up.
- **Automatic login**: Enable this option to allow the specified user to login automatically when the client is starting. Select the auto login user from the drop-down list.
- **Minimize window**: Enable this option to allow the client window to be minimized.
- **Import trusted certificate**: After the Verify Server Cert function is enabled when establishing a connection, click button, and click **Import** on the<Trusted certificate>page to import the authentication certificate for the server. Click **Delete** to delete the trusted certificate in the list.
- **Client certificate management**: Click . On the Client Certificate Management page, click **Import** to import the certificate for login authentication, which is in the PKCS#12 format. You can import GM certificate and non-GM certificate. At most 16 certificate files can be imported. To delete a certificate in the list, click **Delete**.

- Status notification: When the client connection is successful or failed, the corresponding status window appears.

Client Menu

Right-click the green icon of the client, the client menu appears. Descriptions of the menu items:

- **Change Password**: Displays the dialog for changing password.
- **Redirect URL**: When the device end has a redirect URL configured, users can click this menu to quickly jump to this URL address.
- **Resource List**: When accessing the SSL VPN service, user can click this menu to open the browser page displaying internal resources.
- **Application Resource List**: When a user successfully connects to a ZTNA service using the Secure Connect client, this menu is displayed. After the user logs in, a ZTNA portal page will be displayed. The user can click this menu to display the latest ZTNA portal page to view the application resource access privilege after it is closed. The portal page displays the application resources that the user is granted access and is not granted access. For those that the user is not granted access, the user can attempt to acquire the access privilege by adjusting the access terminal configurations. The application resources that the user is denied from accessing will not be displayed on the portal page. If a user is denied from accessing any application resources, the portal page displays a message indicating that no Web resources are available to the user.
- **Show Window**: When Secure Connect client window is minimized, click this menu item to display the client main page.
- **Quit**: Click **Quit** to close the client.

Uninstalling the Client

To uninstall the client from your PC, find and right-click **Hillstone Secure Connect** in the **Start** menu, and then click **Uninstall** in the menu.

L2TP VPN

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

L2TP (Layer Two Tunneling Protocol) is a VPDN technique that allows dial-up users to launch VPN connection from L2TP clients or L2TP access concentrators (LAC), and connect to a L2TP network server (LNS) via PPP. After the connection has been established successfully, LNS will assign IP addresses to legal users and permit them to access the private network.

The device acts as a LNS or a L2TP client in the L2TP tunnel network. When the device acts as a LNS, the device accepts connections from L2TP clients or LACs, implements authentication and authorization, and assigns IP addresses, DNS server addresses and WINS server addresses to legal users.

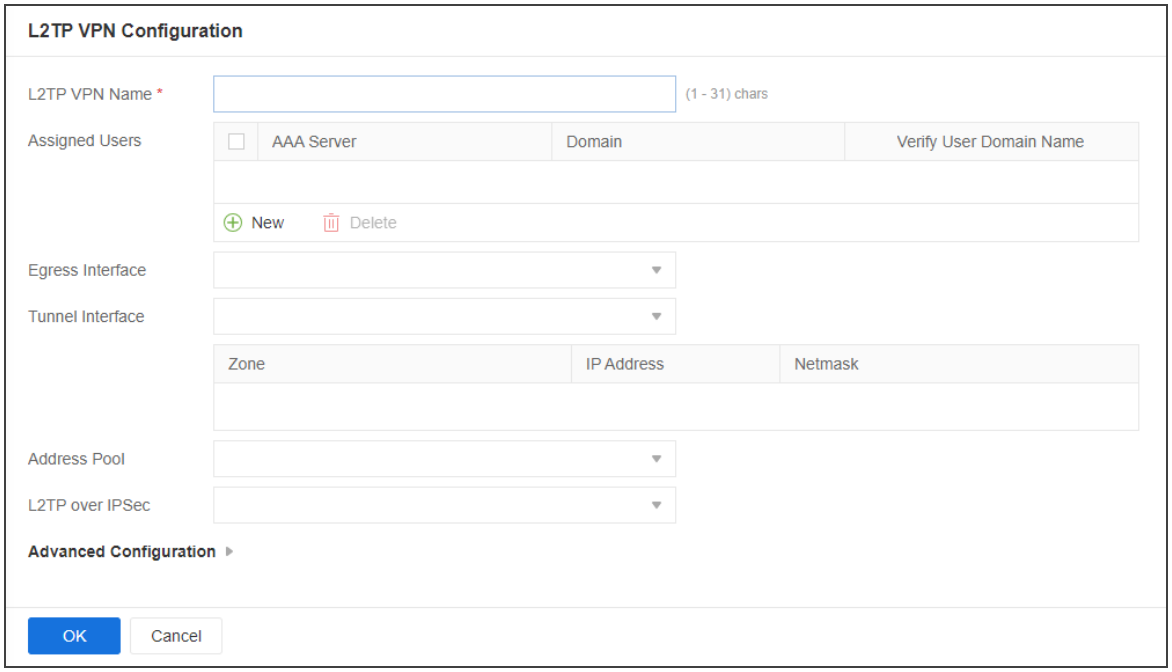
L2TP does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use L2TP in combination with IPsec, and encrypt data by IPSec, thus assuring the security during the data transmitted through the L2TP tunnel.

Configuring a LNS

Configuring an L2TP VPN

To create an L2TP VPN instance, take the following steps:

1. Select **Network > VPN > L2TP VPN**.
2. In the L2TP VPN page, click **New**.



Assigned User	
L2TP VPN Name	Type the name of the L2TP VPN instance.
Assigned Users	Click **New** to add an AAA server. • AAA Server: Select an AAA server from the **AAA Server** drop-down list. • Domain: Type the domain name into the **Domain** box. • Verify User Domain Name: After this function is enable, system will verify the username and its domain name.
Egress Interface	Select the interface from the drop-down list as the L2TP VPN server interface. This interface is used to listen to the request from L2TP clients.

Assigned User	
Tunnel Interface	Specifies the tunnel interface used to bind to the L2TP VPN tunnel. Tunnel interface transmits traffic to/from L2TP VPN tunnel. • Select a tunnel interface from the drop-down list, and then click **Edit** to edit the selected tunnel interface. • Click **New** in the drop-down list to create a new interface.
Information	Shows the zone, IP address, and netmask of the selected tunnel interface.
Address Pool	Specifies the L2TP VPN address pool. • Select an address pool from the drop-down list, and then click **Edit** to edit the selected address pool. • Click **New** in the drop-down list to create a new address pool. For more information about creating/editing address pools, see "Configuring an L2TP VPN Address Pool" on Page 716.
L2TP over IPSec	Select a referenced IPSec tunnel from the drop-down list. L2TP does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use L2TP in combination with IPSec, and encrypt data by IPSec, thus assuring the security for the data transmitted through the L2TP tunnel.

3. If necessary, click **Advanced Configuration** to configure the advanced functions.

   In the Parameters tab, configure the corresponding options.

Security	
Tunnel Authentication	Click **Enable** to enable tunnel authentication to assure the security of the connection. The tunnel authentication can be launched by either LNS or LAC. The tunnel cannot be established unless the both ends are authenticated, i.e., the secret strings of the two ends are consistent.
AVP Hidden	Click **Enable** to enable AVP hidden. L2TP uses AVP (attribute value pair) to transfer and negotiate several L2TP parameters and attributes. By default AVP is transferred in plain text. For data security consideration, you can encrypt the data by the secret string to hide the AVP during the transmission.
Secret	Specifies the secret string that is used for LNS tunnel authentication.
Peer	Specifies the host name of LAC. If multiple LACs are connected to LNS, you can specify different secret strings for different LACs by this parameter.
Add	Click **Add** to add the configured secret and peer name pair to the list.
Client Connection	
Accept Client IP	Click **Enable** to allow the accepting of IP address specified by the client. By default the client IP is selected from the address pool, and allocated by LNS automatically. If this function is enabled, you can specify an IP address. However, this IP address must belong to the specified address pool, and be consistent with the username and role. If the specified IP is already in use, system will not allow the user to log on.
Multiple Login	Click **Enable** to allow a user to log on and be authenticated on different hosts simultaneously.

Security	
Hello Interval	Specifies the interval at which Hello packets are sent. LNS sends Hello packets to the L2TP client or LAC regularly, and will drop the connection to the tunnel if no response is returned after the specified period.
LNS Name	Specifies the local name of LNS.
Tunnel Windows	Specifies the window size for the data transmitted through the tunnel.
Control Packet Transmit Retry	Specifies the retry times of control packets. If no response is received from the peer after the specified retry times, system will determine the tunnel connection is disconnected.
User Going Offline Alarm	Specifies the user going offline alarm profile to monitor the offline status of users. When the number of users going offline exceeds the specified threshold within a specified period of time, the system generates an alarm. From the drop-down list, select a configured user going offline alarm profile, or click ⊕ and create a user going offline alarm profile in the **Going Offline Alarm Configuration** panel. Alternatively, you can hover your mouse over a configured user going offline alarm profile and click ✎ to edit this profile in the **Going Offline Alarm Configuration** panel. For more information about how to create a user going offline alarm profile, see "Creating a User Going Offline Alarm Profile" on Page 973.
PPP Configuration	
LCP Interval Transmit Retries	Specifies parameters for LCP Echo packets used for PPP negotiation. The options are:

Security	
	• Interval: Specifies the interval at which LCP Echo packets are sent. • Transmit Retry: Specifies the retry times for sending LCP Echo packets. If LNS has not received any response after the specified retry times, it will determine the connection is disconnected.
PPP Authentication	Specifies a PPP authentication protocol. The options are: • PAP: Uses PAP for PPP authentication. • CHAP: Uses CHAP for PPP authentication. This is the default option. • Any: Uses CHAP for PPP authentication by default. If CHAP is not supported, then uses PAP.

4. Click **OK** to save the settings.

Configuring an L2TP VPN Address Pool

LNS assigns the IP addresses in the address pool to users. After the client has established a connection to LNS successfully, LNS will choose an IP address along with other related parameters (such as DNS server address, WINS server address, etc) from the address pool, and assign them to the client.

L2TP provides fixed IP addresses by creating and implementing IP binding rules.

- The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, system will assign the binding IP to the client.

- The IP-role binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, system will assign an IP address within the IP range to the client.

When LNS is allocating IP addresses in the address pool, system will check the IP binding rule and determine how to assign IP addresses for the client based on the specific checking order below:



Notes: The IP addresses defined in the static IP binding rule and IP-role binding rule should not be overlapped.

To create an address pool, take the following steps:

1. Select **Network > VPN > L2TP VPN**.
2. At the top-right corner, click **Address Pool**.
3. In the pop-up window, click **New**.

   In the Basic Configuration tab, configure the corresponding options.

Option	Description
Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved Start IP	Specifies the reserved start IP of the address pool.
Reserved End IP	Specifies the reserved end IP of the address pool.
DNS1/2	Specifies the DNS server IP address for the address pool. It is optional. Up to 2 DNS servers can be configured for one address

Option	Description
	pool.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to 2 WIN servers can be configured for one address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the **User** box.
IP	Type the IP address into the **IP** box.
Add	Click **Add** to add this IP user binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Type the role name into the **Role** box.
Start IP	Type the start IP address into the **Start IP** box.
End IP	Type the end IP address into the **End IP** box.
Add	Click **Add** to add this IP role binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.
Up/Down /Top/Bottom	System will query for IP role binding rules by turn, and allocate the IP address according to the first matched rule. You can move the location up or down at your own choice to adjust the

Option	Description
	matching sequence accordingly.

4. Click **OK** to save the settings.

Viewing L2TP VPN Online Users

To view the L2TP VPN online users, take the following steps:

1. Select **Network > VPN > L2TP VPN**.
2. Select an L2TP VPN instance.
3. View the detailed information of the online users in the table.

Option	Description
Name	Displays the name of L2TP VPN.
Login Time	Displays the login time of the L2TP VPN online user.
Public IP	Displays the public IP of the L2TP VPN online user.
Private IP	Displays the private IP of the L2TP VPN online user.
Operation	Displays the executable operation of the L2TP VPN online user.

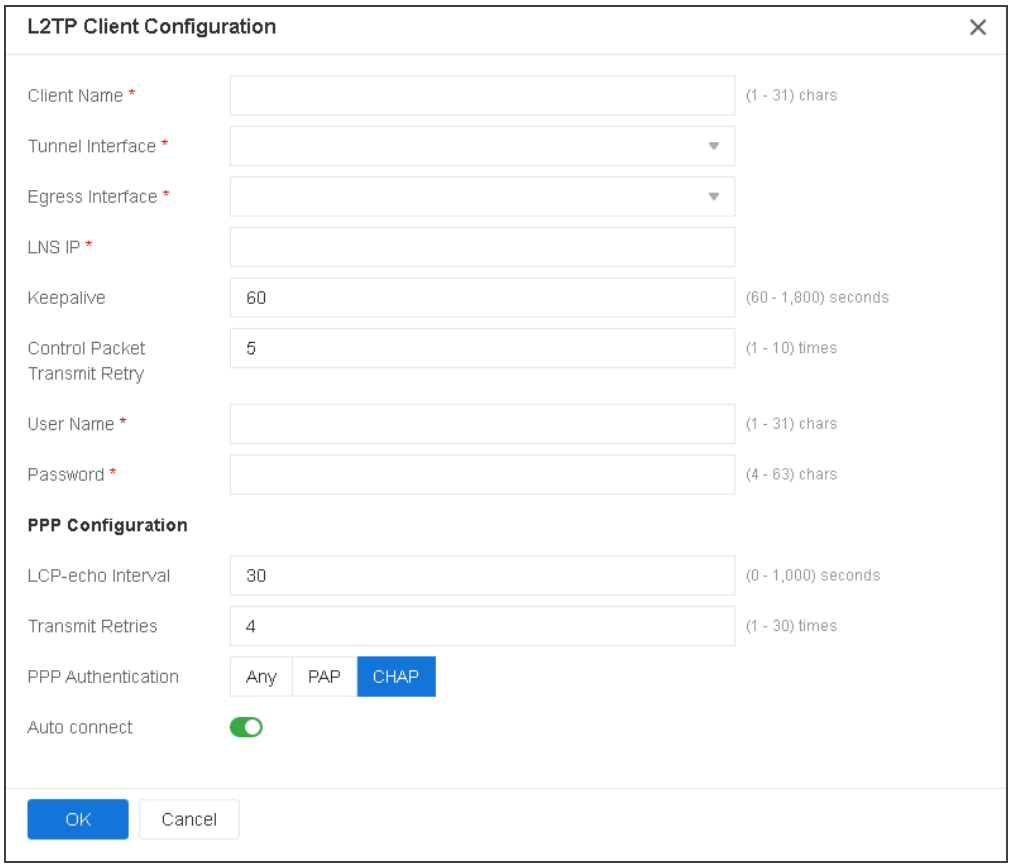
Configuring Device as L2TP Client

Configuring a L2TP Client

To create an L2TP client, take the following steps:

1. Select **Network > VPN > L2TP VPN**.
2. At the top-right corner, click **L2TP Client**.

3. In the L2TP Client page, click **New**.



Option	Description
Client Name	Type the name of the L2TP client.
Tunnel Interface	Specifies the tunnel interface used to bind to the L2TP client. Tunnel interface transmits traffic to/from L2TP client.
Egress Interface	Select the interface from the drop-down list as the L2TP client interface. This interface is used to listen to the request from LNS.
LNS IP	Specifies the IP address of the LNS server.
Keepalive	To ensure normal communication between the LNS and L2TP

Option	Description
	client, the L2TP client periodically sends Hello packets to check whether the LNS is properly connected. Keepalive indicates the interval at which the L2TP client sends two Hello packets. The smaller the value, the quicker the fault sensing; the larger the value, the lower the occupied bandwidths.
Control Packet Transmit Retry	Specifies the retry times of control packets. If no response is received from the peer after the specified retry times, system will determine the tunnel connection is disconnected.
User Name	Specifies the name of the L2TP client, the L2TP client uses the user name to initiate a request to the LNS for establishing an L2TP VPN tunnel.
Password	Specifies the password of the L2TP client.
PPP Configuration	
LCP-echo Interval	Specifies the interval at which LCP Echo packets are sent. The value range is 0 to 1000 seconds.
Transmit Retries	Specifies the retry times for sending LCP Echo packets. If L2TP client has not received any response after the specified retry times, it will determine the connection is disconnected.
PPP Authentication	Specifies a PPP authentication protocol. The options are: • PAP: Uses PAP for PPP authentication. • CHAP: Uses CHAP for PPP authentication. This is the default option.

Option	Description
	• Any: Uses CHAP for PPP authentication by default. If CHAP is not supported, then uses PAP.
Auto connect	Enables the automatic L2TP client dialup function. After the function is enabled, the L2TP client and LNS can establish tunnels. Users can access the intranet connected to the LNS, without performing the PPP dialup.

4. Click **OK**.

VXLAN

Virtual extensible local area network (VXLAN) is a tunnel encapsulation technology for large layer 2 network expansion overe NOV3 that uses MAC-in-UDP encapsulation. VXLAN uses a 24-bit network segment ID, called VXLAN network identifier (VNI), to identify users. This VNI is similar to a VLAN ID and supports a maximum of 16M [(2^24 - 1)/1024^2] VXLAN segments. VXLAN uses MAC-in-UDP encapsulation to extend Layer 2 networks to ensure uninterrupted services during VM migration, the IP address of the VM must remain unchanged.

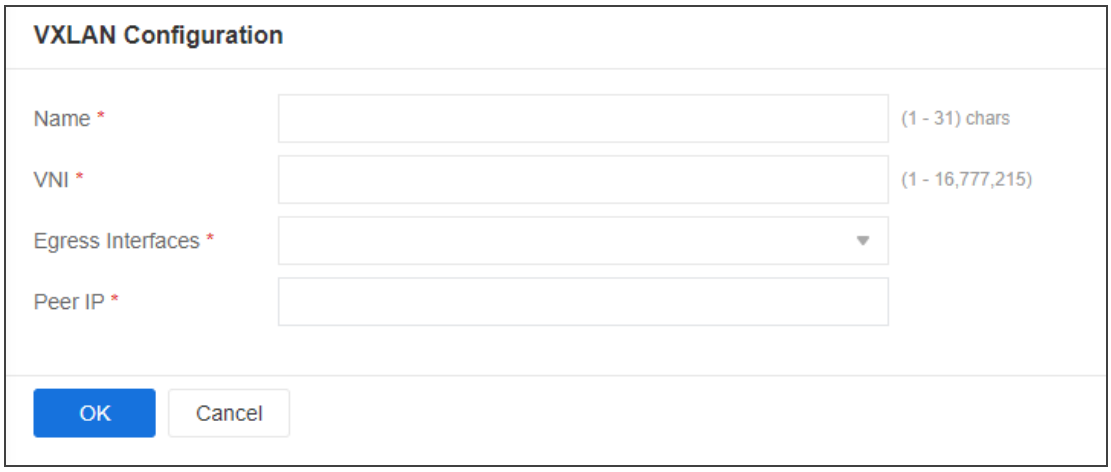
VXLAN uses VTEP (VXLAN Tunnel Endpoint) equipment to encapsulate and decapsulate VXLAN packets, including ARP request packets and normal VXLAN data packets. VTEP encapsulates the original Ethernet frame through VXLAN and sends it to the peer VTEP device. The peer VTEP device decapsulates the VXLAN packet after receiving it, and then forwards it according to the original MAC. The VTEP can be a physical switch, a physical server, or other VXLAN-enabled Hardware equipment or software.

Creating VXLAN Static Tunnel

To creating VXLAN static tunnel, take the following steps:

1. Click **Network > VPN > VXLAN**.

2. Click **New**



Option	Description
Name	Specified the name of the VXLAN static tunnel.
VNI	Specified the ID as the global network identity of the VXLAN network. The value range is 1 to 16777215.
Egress Interfaces	Select the egress interface of the VXLAN network in the drop-down list.
Peer IP	Specified the destination VTEP IP address.

3. Click **OK**.

GRE VPN

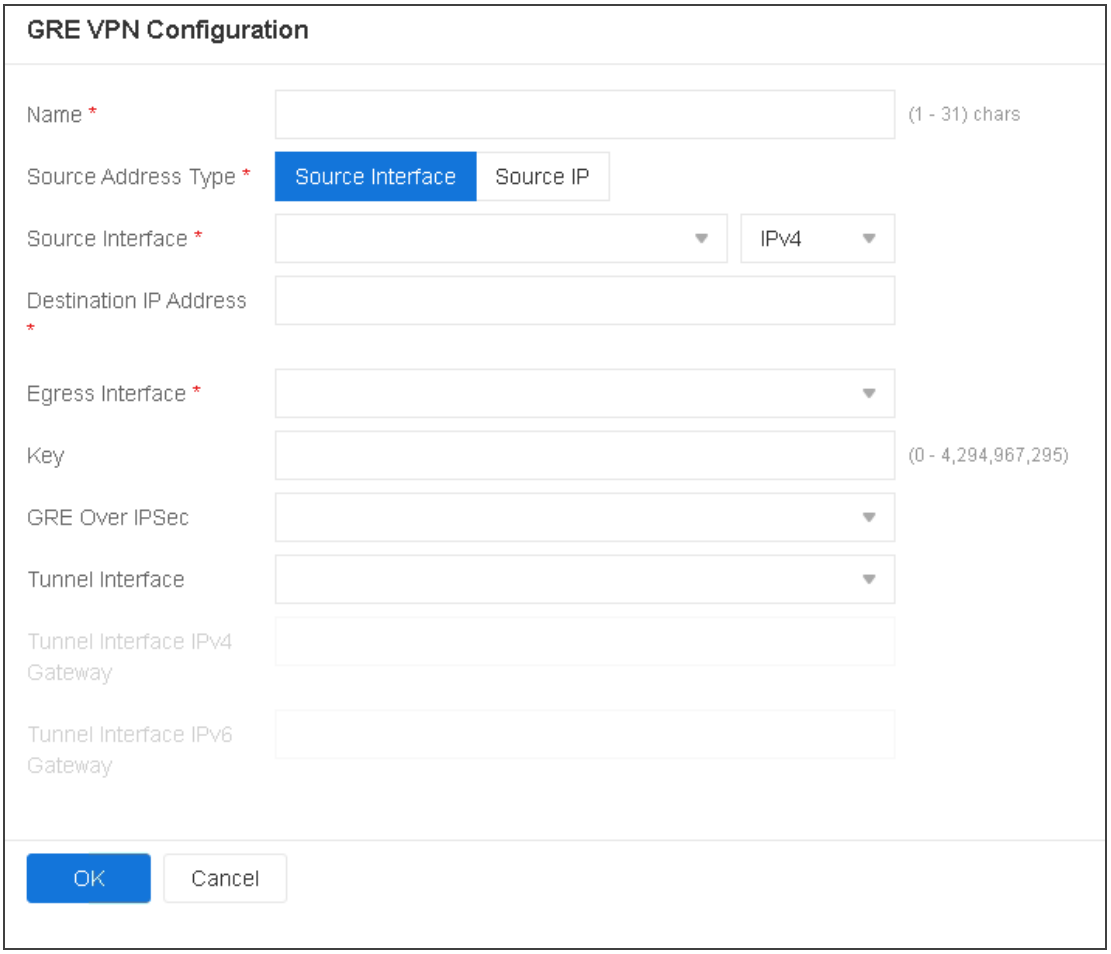
Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol inter-network. StoneOS uses GRE over IPSEC feature to ensure the security of routing information passing between networks.

Configuring GRE VPN

To create an GRE VPN, take the following steps:

1. Select **Network > VPN > GRE VPN**.

2. In the GRE VPN page, click **New**.



Option	Description
Name	Type the name of the GRE VPN.
Source Address Type	Specifies the type of source address for the GRE tunnel.
Source Inter-	Specifies a source interface or source IP Address for the

Option	Description
face/Source IP Address	GRE tunnel.
Destination IP Address	Specifies a destination address for the GRE tunnel
Engress Interface	Select the interface from the drop-down list as the GRE VPN interface.
Key	Specifies the verification key. When the key carried by the packets is the same as the key configured in the receiver, the packets will be decrypted. If the keys are not the same, the packets will be dropped.
GRE Over IPSec	Select a referenced IPSec tunnel from the drop-down list. GRE does not encrypt the data transmitted through the tunnel, so it cannot assure security during the transmission. You can use GRE in combination with IPSec, and encrypt data by IPSec, thus assuring the security for the data transmitted through the GRE tunnel.
Tunnel Interface	Specifies the tunnel interface used to bind to the GRE VPN tunnel. • Select a tunnel interface from the drop-down list, and then click  to edit the selected tunnel interface. • Click  in the drop-down list to create a new interface.
Tunnel Interface	Specifies the next hop (the peer tunnel interface) IP address

Option	Description
IPv4/IPv6 Gate-way	of GRE tunnel when multiple tunnels bind to this interface. The next hop IP addresses can be specified to IPv4 and/or IPv6 addresses.

3. Click **OK**.

Chapter 9 Zero Trust Network Access (ZTNA)

Introduction

Compared with the traditional VPN access mode, which allows an authorized user device to access any resources on the internal network, ZTNA (Zero Trust Network Access) starts with a default deny posture of zero trust on any entities, whether outside or inside the enterprise network perimeter. It grants controlled and least-privilege access to resources after assessment of user identity, device identity and other context-aware attributes, such as access time. It allows users to securely access private applications across clouds and data centers from any location and device.

Hillstone ZTNA solution supports management and control of user access based on dimensions including user identity, device identity and access time and grants access only to specific applications based on adaptive and granular policies. By persistently monitoring the state change of user endpoints, ZTNA solution flexibly adjusts the granted access range. ZTNA login process is as follows:

1. ZTNA user enters the server address, port number, and authentication type (username, username+certificate, certificate, and third-party login) on the client to request authentication and two-step verification, if any.
2. ZTNA server allocates private IP addresses to authenticated users and delivers the endpoint information collection script.
3. ZTNA client executes the script to collect endpoint information, such as OS version, firewall and anti-virus installation information, IE security level, process running, etc. and reports to the ZTNA server.
4. ZTNA server parses endpoint information to obtain the endpoint tag and sends the user name appended with the endpoint tag to the authentication module.

5. Authentication module creates authenticated users, attends the endpoint tag and acquires user group information.
6. ZTNA server matches the user name, user group, endpoint tag and other conditions with ZTNA policies to determine applications that users can access.
7. ZTNA client receives the popped-up ZTNA portal, displaying the icons of application resources that the client is granted and is not granted access. The icons will be displayed with the application resource name and URL address.

ZTNA requires a license to work. The firewall provides 8 concurrent-users authorization by default (128 for X series and K9180). The upper limit for the number of concurrent online ZTNA users varies from hardware platforms. If you want to have a larger user number, consult your local agents to purchase new ZTNA license. For more information about the license, please refer to System Management > License.

ZTNA shares the Hillstone Secure Connect client with SSL VPN. To access ZTNA, please download and install the latest Hillstone Secure Connect client. The client upgrade supports both ZTNA and SSL VPN access. Currently, ZTNA remote access solution supports access from Windows, macOS, Linux, iOS, Android, and ChineseOS endpoints. The firewall supports ZTNA access from Windows, macOS, Linux, iOS, Android and ChineseOS endpoints via corresponding clients. ZTNA intranet access solution supports access from Windows, macOS, Linux, and ChineseOS endpoints. The firewall supports ZTNA access from Windows, macOS, Linux and ChineseOS endpoints via corresponding clients. For information about client installation and usage on these endpoints, refer to:

- Hillstone Secure Connect Client for Windows
- Hillstone Secure Connect Client for macOS
- Hillstone Secure Connect Client for Linux
- Hillstone Secure Connect Client for iOS

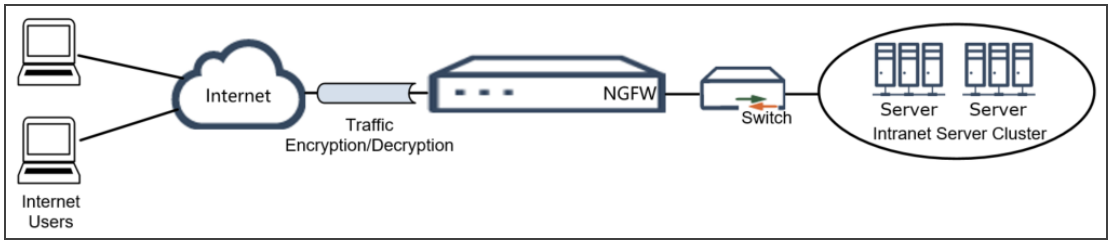
- Hillstone Secure Connect Client for Android
- "Hillstone Secure Connect Client for ChineseOS" on Page 697

ZTNA Typical Scenarios

The typical scenarios of ZTNA include remote access and intranet access.

Remote Access

With the popularity of mobile office, the demand for remote access to intranet resources is growing. To meet this demand and ensure the security of intranet resources, Hillstone provides ZTNA remote access solution. This solution can control access traffic based on remote user identity, status of endpoint device, and access time. It uses fine-grained control policies to enable access to specific authorized applications, and continuously monitors changes in endpoint status to flexibly adjust the scope of authorized applications that users can access.



The user login process for the ZTNA remote access solution is as follows:

1. The ZTNA user enters the server address, port, authentication mode (username/password, username/password + digital certificate, digital certificate only, and third-party application login) on the client, and requests verification. If second-factor authentication is configured, the user needs to complete it.
2. After authentication is passed, the device sends a command to collect endpoint information to the client, assigns a private IP to the client, and establishes a secure tunnel between the device and the client.

3. The client executes the command to collect host information, such as the OS version, whether firewall is installed, antivirus software, browser security level, whether certain processes are running, etc., and reports them to the device.

4. The device parses the host information, obtains endpoint tags, and sends the username and endpoint tags to the authentication module to request the creation of an authenticated user.

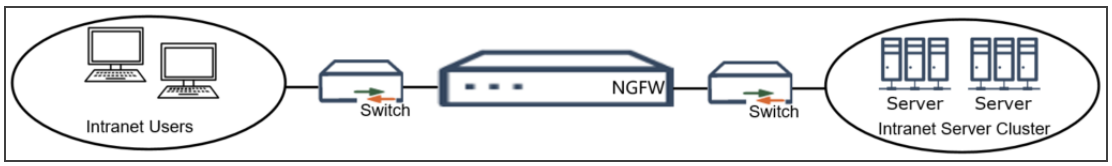
5. The authentication module creates an authenticated user, associates it with endpoint tags, and obtains user group information.

6. Based on the username, user group, and endpoint tags, the device matches the ZTNA policy to determine the list of application resources that the client is allowed to access.

7. The ZTNA client pops up the Portal page, displaying the application resources that the user is allowed and not allowed to access, as well as the names and URLs of the application resources.

Intranet Access

The traditional network security concept assumes that the enterprise intranet is generally secure, and security threats mainly come from the outside. However, many significant security threats often occur within the intranet, such as employees inadvertently downloading malicious software while browsing the internet, posing serious security risks to the entire intranet. In addition, unauthorized access and unauthorized visits within the intranet may lead to business damage and information leakage. To address this issue, Hillstone provides the ZTNA intranet access solution. This solution can control traffic based on the identity of intranet users, status of endpoint device, and access time. It uses fine-grained control policies to enable access to specific authorized applications, and continuously monitors changes in endpoint status to flexibly adjust the scope of authorized applications that users can access.



Compared with the remote access solution, the devices in ZTNA intranet access solution do not need to encrypt and decrypt traffic, so no tunnel needs to be established. The user login process for the ZTNA intranet access solution is as follows:

1. The ZTNA user enters the server address, port, authentication mode (username/password, username/password + digital certificate, digital certificate only, and third-party application login) on the client, and requests verification. If second-factor authentication is configured, the user needs to complete it.
2. After authentication is passed, the device sends a command to collect endpoint information to the client.
3. The client executes the command to collect host information, such as the OS version, whether firewall is installed, antivirus software, browser security level, whether certain processes are running, etc., and reports them to the device.
4. The device parses the host information, obtains endpoint tags, and sends the username and endpoint tags to the authentication module to request the creation of an authenticated user.
5. The authentication module creates an authenticated user, associates it with endpoint tags, and obtains user group information.
6. Based on the username, user group, and endpoint tags, the device matches the ZTNA policy to determine the list of application resources that the client is allowed to access.
7. The ZTNA client pops up the Portal page, displaying the application resources that the user is allowed and not allowed to access, as well as the names and URLs of the application resources.

Configuring ZTNA Gateway

This topic consists of the following sections:

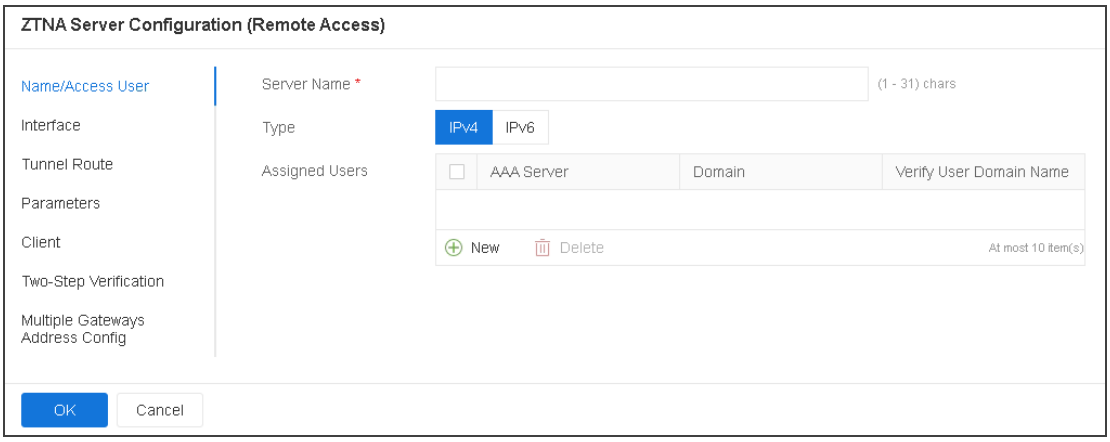
- "Configuring ZTNA Remote Access" on Page 732
- "Configuring ZTNA Intranet Access" on Page 748

Notes: The system allows you to create at most 8 ZTNA gateways. Only one ZTNA gateway can be created in each VSYS, and ZTNA gateway of intranet access cannot be created in non-root VSYS.

Configuring ZTNA Remote Access

To configure ZTNA remote access, take the following steps:

1. Select **ZTNA** > **Gateway**.
2. Click **New** > **Remote Access**.



In the Name/Access User tab, configure the corresponding options.

Option	Description
Server Name	Type the name of the ZTNA instance. The length is 1 to 31 characters.
Type	Select IPv4 or IPv6 to specify the service type of the ZTNA instance. The IPv6 option can only be configured when the version is IPv6.
Assigned Users (at most 10 items)	
AAA Server	Click **New** and select a AAA server from the **AAA Server** drop-down list. Or, you can click **New** in the drop-down list to create an AAA server. If you select an OAuth2 server, the client supports OAuth2 authentication. **Note**: Only Hillstone Secure Connect client for Windows/macOS/Linux/ChineseOS support OAuth2 authentication.
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server. The length is 1 to 31 characters.
Verify User Domain Name	After enabling this function, the system will verify the user name and its domain name. **Note**: The OAuth2 server does not support user domain name verification.

In the Interface tab, configure the corresponding options.

Option	Description
Egress Interface	Specifies the interface used to listen to the request from ZTNA clients. Select the interface from the drop-down list. Or, click **New** in the drop-down list to create an interface. At most 8 interfaces can be selected.
Service Port	Specifies the ZTNA service port number. The value range is 1 to 65535.
Tunnel Interface	Specifies the tunnel interface for the ZTNA instance. Select a tunnel interface from the drop-down list. Or, click **New** in the drop-down list to create a tunnel interface.
Address Pool	Specifies the ZTNA address pool. Select an address pool from the drop-down list. Or, click **New** in the drop-down list to create a new address pool. When configuring IPv6 ZTNA, this option specifies the IPv6 ZTNA address pool.

In the Tunnel Route tab, configure the following options.

Tunnel Route	
A tunnel route created based on a network segment will be distributed to the ZTNA client. ZTNA client uses it to generate the route to the specified destination. A maximum of 128 tunnel routes based on network segments can be added for a ZTNA instance.	
New	Click **New** to add a route.
IP	Type the destination IP address.
Netmask	Type the netmask of the destination IP address.
Metric	Type the metric value. The value range is 1 to 9999.
Type	Sets the user type to **User Group** or **Role**.
User Group/Role	When the type is set to **User Group**, select the AAA server to which the user group belongs and the user group name from the drop-down list. Only users in this user group can access the specified network segment in the tunnel route. You can also click ⊕ and create a user group in the **User Group Configuration** panel. For more information, see Creating a User Group. When the type is set to **Role**, select the role name from the drop-down list. Only users corresponding to this role can access the specified network segment in the tunnel route. You can also click ⊕ and create a role in the **Role Configuration** panel. For more information, see Creating a Role.
Delete	Click **Delete** to delete the selected route.

Tunnel Route	
Add Default Route	Click **Add Default Route** to add a default route with both the IP address and netmask being all 0.

Enable Dedicated ZTNA Tunnel

Click the button to enable the dedicated ZTNA tunnel function. This way, you can access only the internal network resources specified in the tunnel routing but not Internet resources after you log in to ZTNA.



Notes:

- The client versions that support the dedicated ZTNA tunnel function include: the latest version of the ZTNA client for Windows, the latest version of the ZTNA client for macOS, the latest version of the ZTNA client for Linux, and the latest version of the ZTNA client for ChineseOS.
- The dedicated ZTNA tunnel function cannot be used together with the domain route function.
- After you enable the dedicated ZTNA tunnel function, we recommend that you do not configure a default route in the tunnel routing.

Enable Domain Route

After clicking the **Enable** button, the system will distribute the specified domain names to the ZTNA client, and the client will generate the route to the specified destination according to the resolving results from the DNS.

Tunnel Route	
 **Notes:** The domain route function cannot be used together with the dedicated ZTNA tunnel function.	
Maximum	Specifies the maximum numbers of routes that can be generated after obtaining the resolved IP addresses of the domain name. The value range is 1 to 10000. The default value is 1000.
New	Click **New** to add the domain name to the list and you can add up to 64 domain names.
Domain	Specifies the URL of the domain name. The URL cannot exceed 63 characters and it cannot end with a dot. Both wildcards and a single top level domain, e.g. com and .com are not supported.
Delete	Click **Delete** to delete the selected domain name.

In the Parameters tab, configure the corresponding options.

Security Kit	
SSL Version	Specifies the SSL protocol version. The default is TLSv1.2. The option **any** indicates one of TLSv1.0, TLSv1.1, TLSv1.2, TLSv1.3 protocol will be used. If **TLSv1.2** or **any** is specified in ZTNA server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the TLSv1.2 protocol before the digital certificate authentication via ZTNA client, so that the ZTNA server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate. We will take the certificate file named oldcert.pfx as an example, the procedure is as follows: 1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format. **openssl pkcs12 -in oldcert.pfx -out cert.pem** 2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports TLSv1.2 protocol. **openssl pkcs12 -export -in cert.pem -out newcert.pfx -CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"** 3. Import the newly generated .pfx format certificate into

	your browser or USB Key.
Trust Domain	Specifies the PKI trust domain. When the GMSSLv1.0 protocol is used, the specified PKI trust domain needs to include the SM2 signature certificate and its private key for the GMSSL negotiation. The default value is trust_domain_default.
Encryption Trust Domain	When using the GMSSLv1.0 protocol, you must configure this option. The specified encryption PKI trust domain needs to include the SM2 encryption certificate and its private key for the GMSSL negotiation.
Encryption	Specifies the encryption algorithm of the ZTNA tunnel. **NULL** indicates no encryption. When using the GMSSLv1.0 protocol, you're recommended to select SM4 for the encryption algorithm. The default value is AES.
Hash	Specifies the hash algorithm of the ZTNA tunnel. **NULL** indicates no hash. When using the GMSSLv1.0 protocol, you're recommended to select SM3 for the hash algorithm. The default value is MD5.
Compression	Specifies the compression algorithm of the ZTNA tunnel. By default, no compression algorithm is used.
Client Connection	
Allow Download Client from Browser	Select the check box of the client type to specify the allowed type of ZTNA client. By default, you are allowed to access the system with five types of ZTNA clients, which are ZTNA client for Windows, ZTNA client for Android, ZTNA client for iOS, ZTNA client for macOS, and ZTNA client for Linux. You can

	configure to access the system only via the specified types of ZTNA clients as needed.
Idle Time	Specifies the time that a client stays online without any traffic with the server. After waiting for the idle time, the server will disconnect from the client.The value range is 1 minute to 25 hours. The default value is 30 minutes.
Forced Logoff Schedule	Specifies the forced logoff schedule from the drop-down list. When the schedule takes effect, the system forces online ZTNA users to log out based on the periodic schedule or the timeframe. Note: • The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect. • ZTNA users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.
Multiple login	Click **Enable** to permit a user to log in from more than one place simultaneously.
Multiple login times	Specifies the number of simultaneous login with the same user-name. The value range is 0 to 99,999,999. The value 0 indicates that the number of simultaneous login times is not limited. The default value is 0.
Advanced Parameters	
Anti-Replay	The anti-replay function is used to prevent replay attacks. The default value is 32.
DF-Bit	Specifies whether to permit packet fragmentation on the device

	forwarding the packets. The actions include: • Set - Forbids packet fragmentation. • Copy - Copies the DF value from the destination of the packet. It is the default value. • Clear - Permits packet fragmentation.
Port (UDP)	Specifies the UDP port number for the ZTNA connection. The value range is 1 to 65535.
Port (TCP)	Specifies the TCP port number for the ZTNA connection. The value range is 1 to 65535.

In the Client tab, configure the corresponding options.

Client Configuration	
Allowed Client Types	Specifies the ZTNA client types that are allowed to access. By default, the six types of ZTNA clients are allowed to access: Windows, macOS, Linux, ChineseOS, iOS, and Android. You can select one or more client types as required.
Change Password URL	Specifies the URL address where the user will be redirected to modify the password. The length is 0 to 255 characters.
Forgot Password URL	Specifies the URL address where the user will be redirected to reset the password. The length is 0 to 255 characters.
Redirect URL	This function redirects the client to the specified URL address after a successful authentication. The length is 0 to

	255 characters. HTTP (http://) and HTTPS (https://) URLs are supported. Based on the type of the URL, the corresponding fixed format of URL is required. Take the HTTP type as the example: • For the UTF-8 encoding page - The format is URL+username=$USER&password=$PWD, e.g., http://www.- abc.- com/oa/- login.- do?username=$USER&password=$PWD • For the GB2312 page - The format is URL+username=$GBUSER&password=$PWD, e.g., http://www.- 443 Chapter 7 VPN abc.- com/oa/- login.- do?username=$GBUSER&password=$PWD • Other pages: - Type the URL directly, e.g., http://www.abc.com
Title	Specifies description for the redirect URL. The length is 0 to 31 characters. This title will appear as a client menu item.
Client Certificate Authentication	
Authentication	Enable this function to request client certificate authentication. There are two options available: • Username/Password + Digital Certificate - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate, and also type the correct username

	and password. The USB Key certificate users also need to type the USB Key password. • Digital Certificate only - To pass the authentication, you need to have the correct file certificate, or the USB Key that stores the correct digital certificate. The USB Key certificate users also need to type the USB Key password. No username or user's password is required. When **Digital Certificate only** is selected: • System can map corresponding roles for the authenticated users based on the CN or OU field of the USB Key certificate. For more information about the role mapping based on CN or OU, see Role. • System does not allow the local user to change the password. • System does not support SMS authentication. • The client will not re-connect automatically if the USB Key is removed.
USB KEY Download URL	When USB Key authentication is enabled, you can download the UKey driver from this URL. The length 0 to 63 characters.
Trust Domain Subject&Username Checking CN Match-	To configure the trust domain and the subject & username check function: 1. From the **Trust domain** drop-down list, select the

ing OU Matching	PKI trust domain that contains the CA (Certification Authority) certificate. If the client's certificate is the only one that matches to any CA certificate of the trust domain, then the authentication will succeed. 2. If necessary, select the **Subject&Username Checking** check box to enable the subject & username check function. After enabling it, when the user is authenticated by the USB Key certificate, system will check whether the subject CommonName in the client certificate is the same as the name of the login user. You can also enter the strings in the **CN Match** box and the **OU Matching** box to determine whether matches them. 3. You can click **New** to add more items. To delete an item, select the item you want to delete from the list, and then click **Delete**.

In the Two-Step verification tab, configure the corresponding options.

Option	Description
Two-Step Verification	Click **Enable** to enable two-step verification. It means that when a ZTNA user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS authentication, token authentication or email authentication after the username and password are entered. The user must enter the

Option	Description
	random verification code received in order to log in and access intranet resources.
Type	Specifies the verification type, including **SMS Authentication**, **Token Authentication** and **Email Authentication**: • SMS Authentication: Click **SMS Modem** or **SMS Gateway** to specify the authentication type, and configure corresponding options below as needed. • Token Authentication: Click **Token Authentication** and enter the prompt message as needed. The length is 0 to 255 characters. • Email Authentication: Configure corresponding options below as needed.
SMS Authentication	
SMS Auth Type	Select the **SMS Modem** or **SMS Gateway** to specify the SMS authentication type.
SMS Gateway Name	Select the SMS gateway name from the drop-down list. For more information about the SMS gateway, see SMS Gateway.
Lifetime of SMS Verification Code	Specifies the lifetime of the SMS authentication code, in minutes. The value range is 1 to 10. The default value is 10. If the user does not enter the SMS authentication code within the specified time and does not apply for a new code, ZTNA server will disconnect the user.
Sender Name	Specifies a message sender name to display in the message con-

Option	Description
	tent. The length is 0 to 63 characters.  **Notes:** Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.
Verification Code Length	Specifies the length of the SMS verification code. The value range is 4 to 8. The default value is 8.
SMS Temple	Specifies the SMS verification content. The input must contain " $ VRFYCODE" (This parameter is used to get the verification code). "$USERNAME" and "EXPIRATION" are optional. The value range is 9 to 500 characters.
Sign Name	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the sign name must be entered in this field and will be displayed in the message content. The range is 1 to 63 characters. This parameter should be the same with the sign name applied in the ALIYUNSMS.
Template Code	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the code of the SMS template must be entered in this field. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the ALIYUNSMS.
Email Authentication	
Mail Server	Select an existing mail server from the drop-down list. Or, click

Option	Description
	New to create a mail server. For more information about the configuration of a mail server, see Mail Server.
Lifetime of Email Verification Code	Specifies the lifetime of the Email verification code, in minutes. The value range is 1 to 10. The default value is 10. Each Email verification code has a period of validity. If the user neither types the verification code within the period nor applies for a new code, ZTNA server will disconnect the connection.
Sender Name	Specifies a verification code sender name to display in the Email content. The range is 0 to 63 characters. In order to prevent the mail from being identified as spam, it's recommended that users configure the sender name.
Verification Code Length	Specifies the length of the Email verification code. The value range is 4 to 8 . The default value is 8.
Email Verification Content	Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The length is 18 to 128 characters. The default content is "SSL VPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.".
Multiple Gateways Address Config	
When the ZTNA service is enabled for multiple devices in the network, you can add the service addresses (egress interface addresses or domain names) of these devices to the gateway address list. When the client establishes a ZTNA con-	

Option	Description
nection with the device, it can select the address with the best link quality from the list to establish the connection. When the device is configured with a gateway address list, the client can enable gateway detection function to select the desired ZTNA gateway for connection.	
Name	Click **New** to add a gateway address configuration in the gateway address list. Enter the gateway name. The range is 1 to 31 characters. Up to 24 gateways can be configured. When you configure multiple gateways, the ZTNA configurations on the multiple gateways need to be the same as those on the master ZTNA gateway.
Gateway Address	Specifies the IPv4 address or domain name of multiple gateways. The range for a domain is 255 characters and the maximum length between the two periods (.) cannot exceed 63 characters.

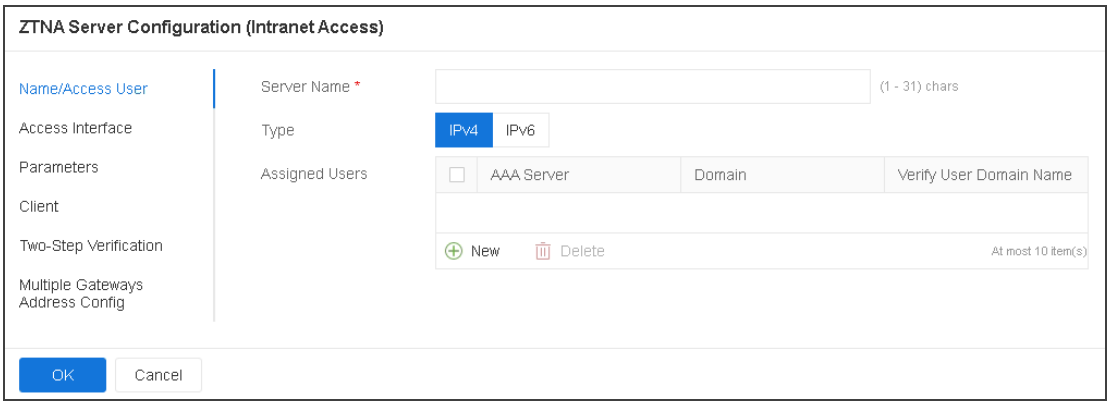
2. Click **OK** to save the settings.

Configuring ZTNA Intranet Access

To configure ZTNA intranet access, take the following steps:

1. Select **ZTNA** > **Gateway**.

2. Click **New** > **Intranet Access**.



In the Name/Access User tab, configure the corresponding options.

Option	Description
Server Name	Type the name of the ZTNA instance. The length is 1 to 31 characters.
Type	Select IPv4 or IPv6 to specify the service type of the ZTNA instance. The IPv6 option can only be configured when the version is IPv6.
Assigned Users (at most 10 items)	
AAA Server	Click **New** and select a AAA server from the **AAA Server** drop-down list. Or, you can click **New** in the drop-down list to create an AAA server. **Note**: Only Hillstone Secure Connect client for Windows/macOS/Linux/ChineseOS support OAuth2 authentication.
Domain	Type the domain name into the **Domain** box. The domain name is used to distinguish the AAA server. The length is 1 to 31 characters.
Verify User Domain Name	After enabling this function, the system will verify the user name and its domain name. **Note**: The OAuth2 server does not support user domain name verification.

In the Interface tab, configure the corresponding options.

Option	Description
Egress Interface	Specifies the interface used to listen to the request from ZTNA clients. Select the interface from the drop-down list. Or, click

Option	Description
	New in the drop-down list to create an interface. At most 8 interfaces can be selected.
Service Port	Specifies the ZTNA service port number. The value range is 1 to 65535.

In the Parameters tab, configure the corresponding options.

Security Kit	
SSL Version	Specifies the SSL protocol version. The default is TLSv1.2. The option **any** indicates one of TLSv1, TLSv1.1, TLSv1.2, TLSv1.3 protocol will be used. If **TLSv1.2** or **any** is specified in ZTNA server, you need to convert the certificate that you are going to import to the browser or certificate in the USB Key to make it support the TLSv1.2 protocol before the digital certificate authentication via ZTNA client, so that the ZTNA server can be connected successfully when the Username/Password + Digital Certificate or Digital Certificate Only authentication method is selected. Prepare a PC with Windows or Linux system which has been installed with OpenSSL 1.0.1 or later before processing the certificate. We will take the certificate file named oldcert.pfx as an example, the procedure is as follows: 1. In the OpenSSL software interface, enter the following command to convert a certificate in .pfx format to a certificate in .pem format. **openssl pkcs12 –in oldcert.pfx –out cert.pem** 2. Enter the following command to convert the certificate in .pem format to a .pfx format certificate that supports TLSv1.2 protocol. **openssl pkcs12 –export –in cert.pem –out newcert.pfx –CSP "Microsoft Enhanced RSA and AES Cryptographic Provider"** 3. Import the newly generated .pfx format certificate into

Security Kit	
	your browser or USB Key.
Trust Domain	Specifies the PKI trust domain. When the GMSSLv1.0 protocol is used, the specified PKI trust domain needs to include the SM2 signature certificate and its private key for the GMSSL negotiation. The default value is trust_domain_default.
Encryption Trust Domain	When using the GMSSLv1.0 protocol, you must configure this option. The specified encryption PKI trust domain needs to include the SM2 encryption certificate and its private key for the GMSSL negotiation.
Client Connection	
Allow Down-load Client from Browser	After you enable this function, you can download the Hillstone Secure Connect client on the Web page of the browser. By default, this function is enabled. When disabled, you can only download the Hillstone Secure Connect client from the official website of Hillstone Networks. Note: The method to download the client via the browser is as follows: "https://IP-Address:Port-Number", where "IP-Address" is the IP address configured for the egress interface in the Interface tab and "Port-Number" is the service port con-figured here.
Forced Timeout	Specifies the time that a client stays online. After waiting for the time, the server will disconnect from the client. The value range is 10 minutes to 7 days. The default value is 7 days.
Forced Logoff	Specifies the forced logoff schedule from the drop-down list.

Security Kit	
Schedule	When the schedule takes effect, the system forces online ZTNA users to log out based on the periodic schedule or the timeframe. Note: • The start time cannot be the same as the end time. If they are the same, the timeframe cannot take effect. • ZTNA users who log in after the forced logoff schedule takes effect will be forced to log out when the schedule takes effect next time.
Multiple login	Click **Enable** to permit a user to log in from more than one place simultaneously.
Multiple login times	Specifies the number of simultaneous login with the same user-name. The value range is 0 to 99,999,999. The value 0 indicates that the number of simultaneous login times is not limited. The default value is 0.

In the Client tab, configure the corresponding options.

Client Configuration	
Allowed Client Types	Specifies the ZTNA client types that are allowed to access. By default, the three types of ZTNA clients are allowed to access: Windows, macOS, Linux. You can select one or more client types as required.
Change Pass-word URL	Specifies the URL address where the user will be redirected to modify the password. The length is 0 to 255 characters.
Forgot Pass-	Specifies the URL address where the user will be redirected to

Client Configuration	
word URL	reset the password. The length is 0 to 255 characters.
Redirect URL	This function redirects the client to the specified URL address after a successful authentication. The length is 0 to 255 characters. HTTP (http://) and HTTPS (https://) URLs are supported. Based on the type of the URL, the corresponding fixed format of URL is required. Take the HTTP type as the example: • For the UTF-8 encoding page - The format is URL+username=$USER&password=$PWD, e.g., http://www.-abc.- com/oa/- login.-do?username=$USER&password=$PWD • For the GB2312 page - The format is URL+username=$GBUSER&password=$PWD, e.g., http://www.- 443 Chapter 7 VPN abc.- com/oa/-login.- do?username=$GBUSER&password=$PWD • Other pages: - Type the URL directly, e.g., http://www.-abc.com
Title	Specifies description for the redirect URL. The length is 0 to 31 characters. This title will appear as a client menu item.
Client Certificate Authentication	
Authentication	Enable this function to request client certificate authentication. There are two options available: "Username/Password + Digital Certificate" and "Digital Certificate only". When **Digital**

Client Configuration	
	Certificate only is selected: • System can map corresponding roles for the authenticated users based on the CN or OU field of the USB Key certificate. For more information about the role mapping based on CN or OU, see Role. • System does not allow the local user to change the password. • System does not support SMS authentication. • The client will not re-connect automatically if the USB Key is removed.
USB KEY Download URL	When USB Key authentication is enabled, you can download the UKey driver from this URL. The length 0 to 63 characters.
Trust Domain	To configure the trust domain and the subject & username check function: 1. From the **Trust domain** drop-down list, select the PKI trust domain that contains the CA (Certification Authority) certificate. If the client's certificate is the only one that matches to any CA certificate of the trust domain, then the authentication will succeed. 2. If necessary, select the **Subject&Username Checking** check box to enable the subject & username check function. After enabling it, when the user is authenticated by the USB Key certificate, system will check

Client Configuration	
	whether the subject CommonName in the client certificate is the same as the name of the login user. You can also enter the strings in the **CN Match** box and the **OU Matching** box to determine whether matches them. 3. You can click **New** to add more items. To delete an item, select the item you want to delete from the list, and then click **Delete**.

In the Two-Step verification tab, configure the corresponding options.

Option	Description
Two-Step Verification	Click **Enable** to enable two-step verification. It means that when a ZTNA user logs in by providing a "username/password" or a "username/password+Digital Certificate", the Hillstone device will implement the two-step verification by means of SMS authentication, token authentication or email authentication after the username and password are entered. The user must enter the random verification code received in order to log in and access intranet resources.
Type	Specifies the verification type, including **SMS Authentication**, **Token Authentication** and **Email Authentication**: • SMS Authentication: Click **SMS Modem** or **SMS Gateway** to specify the authentication type, and configure corresponding options below as needed.

Option	Description
	• Token Authentication: Click **Token Authentication** and enter the prompt message as needed. The length is 0 to 255 characters. • Email Authentication: Configure corresponding options below as needed.
SMS Authentication	
SMS Auth Type	Select the **SMS Modem** or **SMS Gateway** to specify the SMS authentication type.
SMS Gateway Name	Select the SMS gateway name from the drop-down list. For more information about the SMS gateway, see SMS Gateway.
Lifetime of SMS Verification Code	Specifies the lifetime of the SMS authentication code, in minutes. The value range is 1 to 10. The default value is 10. If the user does not enter the SMS authentication code within the specified time and does not apply for a new code, ZTNA server will disconnect the user.
Sender Name	Specifies a message sender name to display in the message content. The length is 0 to 63 characters. **Notes:** Due to the limitation of UMS enterprise information platform, when the the SMS gateway authentication is enabled, the sender name will be displayed on the name of the UMS enterprise information platform.
Verification Code Length	Specifies the length of the SMS verification code. The value range is 4 to 8. The default value is 8.

Option	Description
SMS Temple	Specifies the SMS verification content. The input must contain " $ VRFYCODE" (This parameter is used to get the verification code). "$USERNAME" and "EXPIRATION" are optional. The value range is 9 to 500 characters.
Sign Name	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the sign name must be entered in this field and will be displayed in the message content. The range is 1 to 63 characters. This parameter should be the same with the sign name applied in the ALIYUNSMS.
Template Code	If an ALIYUNSMS service provider name is specified for the **SMS Gateway Name** option, the code of the SMS template must be entered in this field. The range is 1 to 30 characters. This parameter should be the same with the template code applied in the ALIYUNSMS.
Email Authentication	
Mail Server	Select an existing mail server from the drop-down list. Or, click **New** to create a mail server. For more information about the configuration of a mail server, see Mail Server.
Lifetime of Email Verification Code	Specifies the lifetime of the Email verification code, in minutes. The value range is 1 to 10. The default value is 10. Each Email verification code has a period of validity. If the user neither types the verification code within the period nor applies for a new code, ZTNA server will disconnect the connection.
Sender Name	Specifies a verification code sender name to display in the

Option	Description
	Email content. The range is 0 to 63 characters. In order to prevent the mail from being identified as spam, it's recommended that users configure the sender name.
Verification Code Length	Specifies the length of the Email verification code. The value range is 4 to 8 . The default value is 8.
Email Verification Content	Specifies the Email verification content. The input must contain " $ USERNAME" (This parameter is used to get the username) and " $ VRFYCODE" (This parameter is used to get the verification code). The length is 18 to 128 characters. The default content is "SSL VPN user < $ USERNAME> email verification code: $ VRFYCODE. Do not reveal to anyone! If you did not request this, please ignore it.".

Multiple Gateways Address Config

Option	Description
When the ZTNA service is enabled for multiple devices in the network, you can add the service addresses (egress interface addresses or domain names) of these devices to the gateway address list. When the client establishes a ZTNA connection with the device, it can select the address with the best link quality from the list to establish the connection. When the device is configured with a gateway address list, the client can enable gateway detection function to select the desired ZTNA gateway for connection.	
Name	Click **New** to add a gateway address configuration in the gateway address list. Enter the gateway name. The range is 1 to 31 characters. Up to 24 gateways can be configured. When you con-

Option	Description
	figure multiple gateways, the ZTNA configurations on the multiple gateways need to be the same as those on the master ZTNA gateway.
Gateway Address	Specifies the IPv4 address or domain name of multiple gateways. The range for a domain is 255 characters and the maximum length between the two periods (.) cannot exceed 63 characters.

2. Click **OK**.

Managing Endpoint Items

Introduction

Endpoint item management enables you to configure endpoint information collection, generate and deploy the endpoint information collection script, and constantly monitor the endpoint status. After a client logs in, the system will continuously monitor the endpoint state and update the attended endpoint tag and the granted resource access range, no matter whether the client accesses resources. The monitoring process is as follows:

1. The client periodically collects endpoint information based on the collection script and reports to the ZTNA server. By default, the client collects and reports collected endpoint information at the interval of 60 minutes. The interval can be modified as required via the **ztna-endpoint-information-monitor** command.
2. ZTNA server parses the received endpoint information and re-acquires the endpoint tag if the endpoint state changes. Then the endpoint tag attended to the authorized user will be updated, the ZTNA policy is re-matched and the resource access range granted to the user is

updated as well. For existing sessions of this user, the system will process them based on the configuration of the **session-rematch** command.

Endpoint items include the predefined and custom ones. The predefined endpoint items are supported by the system by default and cannot be edited. You can add custom types to collect more endpoint items, so that ZTNA can obtain more endpoint information for better access control.

The system supports endpoint item management of the following operating systems:

- Windows endpoint item management
- macOS endpoint item management
- Linux endpoint item management
- ChineseOS endpoint item management
- iOS endpoint item management
- Android endpoint item management

Windows Endpoint Item Management

To manage Windows endpoint items, take the following steps

1. Select **ZTNA** > **Endpoint** > **Information** > **Windows**.



2. View the Window endpoint items that the system support to collect and configure custom items.

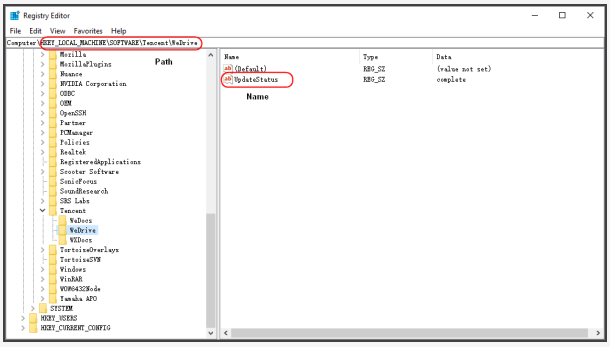
Windows Endpoint Items - Predefined

Option	Description
OS Version	Checks the OS version of the Windows endpoint. Click **OS Version** to view the Windows versions that the system supports to check, including: • Windows 7/8.1/10/11 • Windows server 2008 R2/2012/2012 R2/2016/2019/2022
IE	Checks the IE version and security level of the Windows endpoint. Click **IE** to view the IE versions and IE security levels that the system supports to collect: • IE Version: IE7 ~ IE11 • IE Security Level: custom define, low, medium low, medium, medium high, high
Security Center	Checks the system security of the Windows endpoint. Click **Security Center** to view the security items that the system supports to check: • Whether anti-spyware software is installed, enabled and updated. • Whether anti-virus software is installed, enabled and updated.

Option	Description
	• Whether firewall software is installed and enabled. • Whether windows-update is enabled.

Windows Endpoint Items - Custom

Option	Description
Hotfix	Checks whether the specified hot fix is installed in the Windows endpoint. You can add up to 5 hot fixes as Windows endpoint items. Click **Hotfix** and then **New** on the Hotfix page. Define hot fix information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the hot fix's alias. The length is 1 to 31 characters. • Hotfix: Specify the actual name of the hot fix. The length is 1 to 255 characters.
Registry Key	Checks whether the specified registry key exists in the Windows endpoint. You can add up to 5 registry keys as Windows endpoint items. Click **Registry Key** and then **New** on the Registry Key page. Define registry key information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the registry key's alias. The length is 1 to 31 characters. • Key: Specify the actual name of the registry key. The length is 1 to 255 characters. The content filled in the text box is "key path + name". For example, in the following figure, the content filled in is HKEY_ LOCAL_ Machine\Software\Tencent \ WeDrive\UpdateStatus.

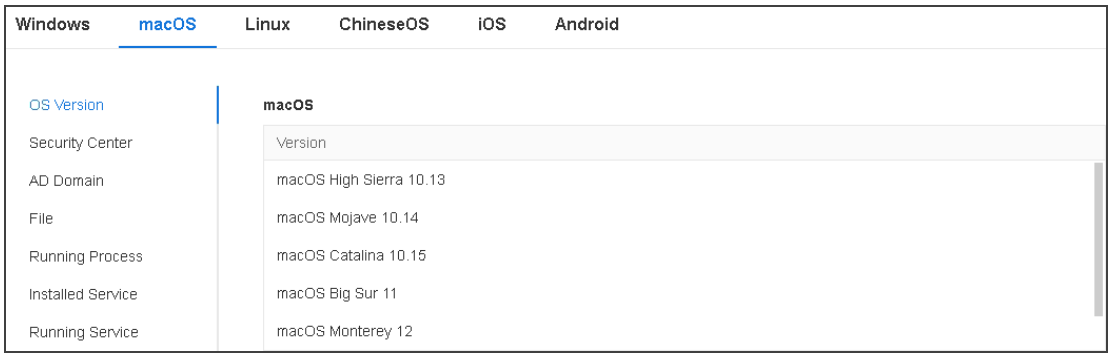
Option	Description
	
File	Checks whether the specified file exists in the Windows endpoint. You can add up to 5 files as endpoint items. Click **File** and then **New** on the File page. Define file information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the file's alias. The length is 1 to 31 characters. • File Path: Specify the file's absolute path. The length is 1 to 255 characters.
Running Process	Checks whether the specified process is running in the Windows endpoint. You can add up to 5 running processes as Windows endpoint items. Click **Running Process** and then **New** on the Running Process page. Define process information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the process's alias. The length is 1 to 31 characters. • Running Process: Specify the actual name of the pro-

Option	Description
	cess. The length is 1 to 255 characters.
Installed Service	Checks whether the specified service is installed in the Windows endpoint. You can add up to 5 installed services as Windows endpoint items. Click **Installed Service** and then **New** on the Installed Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Installed Service: Specify the actual name of the service. The length is 1 to 255 characters.
Running Service	Checks whether the specified service is running in the Windows endpoint. You can add up to 5 running services as Windows endpoint items. Click **Running Service** and then **New** on the Running Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Running Service: Specify the actual name of the service. The length is 1 to 255 characters.

macOS Endpoint Item Management

To manage macOS endpoint items, take the following steps

1. Select **ZTNA** > **Endpoint** > **Information** > **macOS**.



2. View the macOS endpoint items that the system support to collect and configure custom items.

   macOS Endpoint Items - Predefined

Option	Description
OS Version	Checks the OS version of the macOS endpoint. Click **OS Version** to view the macOS versions that the system supports to check, including: • macOS High Sierra 10.13 • macOS Mojave 10.14 • macOS Catalina 10.15 • macOS Big Sur 11 • macOS Monterey 12 • macOS Ventura 13
Security Center	Checks the system security of the macOS endpoint. Click **Security Center** to view the security items that the system supports to check, that is, whether FileVault is enabled.

macOS Endpoint Items - Custom

Option	Description
AD Domain	Checks the AD domain name of the macOS endpoint. You can add one AD domain name as the macOS endpoint item. Click **AD Domain** and then **New** on the AD Domain page. Define AD Domain information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the AD domain name's alias. The length is 1 to 31 characters. • AD Domain: Specify the AD domain name. The length is 1 to 255 characters.
File	Checks whether the specified file exists in the macOS endpoint. You can add up to 5 files as macOS endpoint items. Click **File** and then **New** on the File page. Define file information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the file's alias. The length is 1 to 31 characters. • File Path: Specify the file's absolute path. The length is 1 to 255 characters.
Running Process	Checks whether the specified process is running in the macOS endpoint. You can add up to 5 running processes as macOS endpoint items. Click **Running Process** and then **New** on the Running Process page. Define process inform-

Option	Description
	ation that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the process's alias. The length is 1 to 31 characters. • Running Process: Specify the actual name of the process. The length is 1 to 255 characters.
Installed Service	Checks whether the specified service is installed in the macOS endpoint. You can add up to 5 installed services as macOS endpoint items. Click **Installed Service** and then **New** on the Installed Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Installed Service: Specify the actual name of the service. The length is 1 to 255 characters.
Running Service	Checks whether the specified service is running in the macOS endpoint. You can add up to 5 running services as macOS endpoint items. Click **Running Service** and then **New** on the Running Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31

Option	Description
	characters. • Running Service: Specify the actual name of the service. The length is 1 to 255 characters.

Linux Endpoint Item Management

To manage Linux endpoint items, take the following steps

1. Select **ZTNA** > **Endpoint** > **Information** > **Linux**.



2. View the Linux endpoint items that the system support to collect and configure custom items.

Linux Endpoint Items - Predefined

Option	Description
OS Version	Checks the OS version of the Linux endpoint. Click **OS Version** to view the Linux versions that the system supports to check, including: • CentOS 7.6/7.7/7.8/7.9/8.0/8.1/8.2/8.3/8.4/8.5 • Ubuntu 18.04/18.10/19.04/19.10/20.04/20.10/21.04

Option	Description
	• Ubuntu Kylin 18.04/20.04

Linux Endpoint Items - Custom

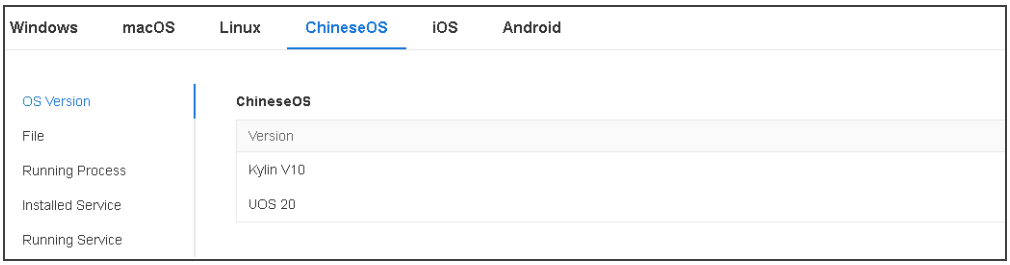
Option	Description
File	Checks whether the specified file exists in the Linux endpoint. You can add up to 5 files as Linux endpoint items. Click **File** and then **New** on the File page. Define file information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the file's alias. The length is 1 to 31 characters. • File Path: Specify the file's absolute path. The length is 1 to 255 characters.
Running Process	Checks whether the specified process is running in the Linux endpoint. You can add up to 5 running processes as Linux endpoint items. Click **Running Process** and then **New** on the Running Process page. Define process information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the process's alias. The length is 1 to 31 characters. • Running Process: Specify the actual name of the process. The length is 1 to 255 characters.
Installed Service	Checks whether the specified service is installed in the Linux endpoint. You can add up to 5 installed services as Linux endpoint items. Click **Installed Service** and then **New**

Option	Description
	on the Installed Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Installed Service: Specify the actual name of the service. The length is 1 to 255 characters.
Running Service	Checks whether the specified service is running in the Linux endpoint. You can add up to 5 running services as Linux endpoint items. Click **Running Service** and then **New** on the Running Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Running Service: Specify the actual name of the service. The length is 1 to 255 characters.

ChineseOS Endpoint Item Management

To manage ChineseOS endpoint items, take the following steps:

1. Select **ZTNA** > **Endpoint** > **Information** > **ChineseOS**.



2. View the ChinesOS endpoint items that the system support to collect and configure custom items.

ChineseOS Endpoint Items - Predefined

Option	Description
OS Version	Collects the versions of ChineseOS. Click **OS Version** to view ChineseOS versions that the system supports to check, including: • Kylin V10 • UOS 20

ChineseOS Endpoint Items - Custom

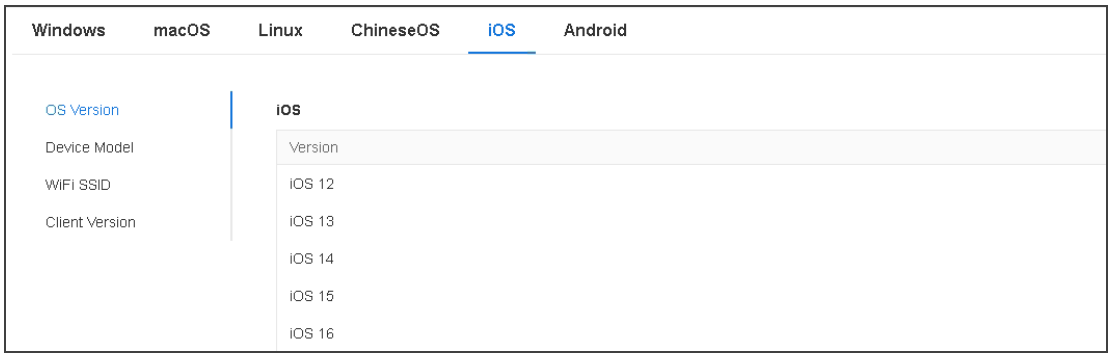
Option	Description
File	Checks whether the specified file exists in the ChineseOS endpoint. You can add up to 5 files as ChineseOS endpoint items. Click **File** and then **New** on the File page. Define file information that needs to be collected and then click **OK** to save the configuration. • lias: Specify the file's alias. The length is 1 to 31 characters. • File Path: Specify the file's absolute path. The length is 1 to 255 characters.
Running Process	Checks whether the specified process is running in the ChineseOS endpoint. You can add up to 5 running processes as ChineseOS endpoint items. Click **Running Process** and then **New** on the Running Process page. Define process information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the process's alias. The length is 1 to 31 characters. • Running Process: Specify the actual name of the process. The length is 1 to 255 characters.
Installed Service	Checks whether the specified service is installed in the ChineseOS endpoint. You can add up to 5 installed services as ChineseOS endpoint items. Click **Installed Service** and then **New** on the Installed Service page. Define service information

Option	Description
	that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Installed Service: Specify the actual name of the service. The length is 1 to 255 characters.
Running Service	Checks whether the specified service is running in the ChineseOS endpoint. You can add up to 5 running services as ChineseOS endpoint items. Click **Running Service** and then **New** on the Running Service page. Define service information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the service's alias. The length is 1 to 31 characters. • Running Service: Specify the actual name of the service. The length is 1 to 255 characters.

iOS Endpoint Item Management

To manage iOS endpoint items, take the following steps

1. Select **ZTNA** > **Endpoint** > **Information** > **iOS**.



2. View the iOS endpoint items that the system support to collect and configure custom items.

   iOS Endpoint Items - Predefined

Option	Description
OS Version	Checks the OS version of the iOS endpoint. Click **OS Version** to view the iOS versions that the system supports to check, including iOS 12/13/14/15/16.

iOS Endpoint Items - Custom

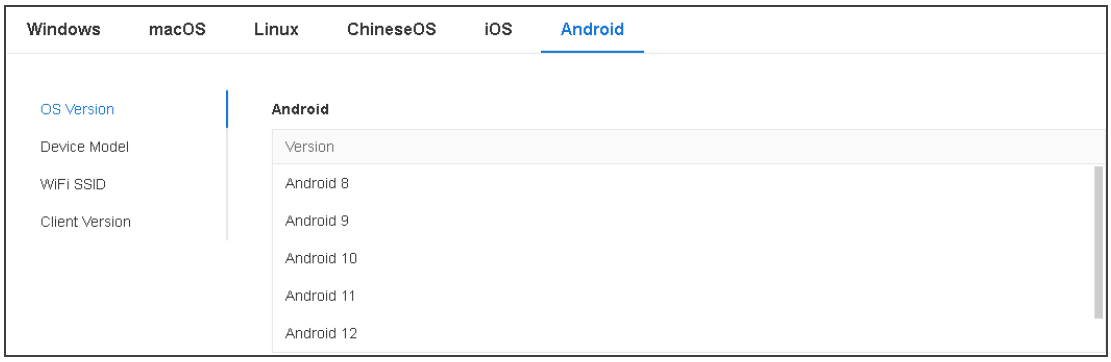
Option	Description
Device Model	Checks the device model of the iOS endpoint. You can add up to 5 device model numbers as iOS endpoint items. Click **Device Model** and then **New** on the Device Model page. Define device model information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the iOS device model's alias. The length is 1 to 31 characters. • Device Model: Specify the iOS device model number. The length is 1 to 255 characters.
WiFi SSID	Checks the connected WiFi SSID of the iOS endpoint. You can add up to 5 WiFi SSIDs as iOS endpoint items. Click **WiFi SSID** and then **New** on the WiFi SSID page. Define WiFi SSID information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the WiFi SSID's alias. The length is 1 to 31 characters. • WiFi SSID: Specify the WiFi SSID. The length is 1 to 255 characters.
Client Version	Checks the ZTNA client version of the iOS endpoint. You can add up to 5 ZTNA client versions as iOS endpoint items. Click **Client Version** and then **New** on the Client Version page. Define ZTNA client Version information that

Option	Description
	needs to be collected and then click **OK** to save the configuration. • Alias: Specify the client version's alias. The length is 1 to 31 characters. • Client Version: Specify the client version. The length is 1 to 255 characters.

Android Endpoint Item Management

To manage Android endpoint items, take the following steps

1. Select **ZTNA** > **Endpoint** > **Information** > **Android**.



2. View the Android endpoint items that the system support to collect and configure custom items.

Android Endpoint Items - Predefined

Option	Description
OS Version	Checks the OS version of the Android endpoint. Click **OS Version** to view the Android versions that the system supports to check, including Android 8/9/10/11/12/13.

Android Endpoint Items - Custom

Option	Description
Device Model	Checks the device model of the Android endpoint. You can add up to 5 device model numbers as Android endpoint items. Click **Device Model** and then **New** on the Device Model page. Define device model information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the Android device model's alias. The length is 1 to 31 characters. • Device Model: Specify the Android device model number. The length is 1 to 255 characters.
WiFi SSID	Checks the connected WiFi SSID of the Android endpoint. You can add up to 5 WiFi SSIDs as Android endpoint items. Click **WiFi SSID** and then **New** on the WiFi SSID page. Define WiFi SSID information that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the WiFi SSID's alias. The length is 1 to 31 characters. • WiFi SSID: Specify the WiFi SSID. The length is 1 to 255 characters.
Client Version	Checks the ZTNA client version of the Android endpoint. You can add up to 5 ZTNA client versions as Android endpoint items. Click **Client Version** and then **New** on the Client Version page. Define ZTNA client Version information

Option	Description
	that needs to be collected and then click **OK** to save the configuration. • Alias: Specify the client version's alias. The length is 1 to 31 characters. • Client Version: Specify the client version. The length is 1 to 255 characters.

Endpoint Tags

Introduction

Endpoint tags are used to identify the endpoint status information of users. The system assigns corresponding endpoint tags to users based on the endpoint information carried by the users. These tags are used as matching conditions for ZTNA policies. Users with specific tags are granted access only to specific resources. This way, ZTNA enables the inspection and control of user access privileges.

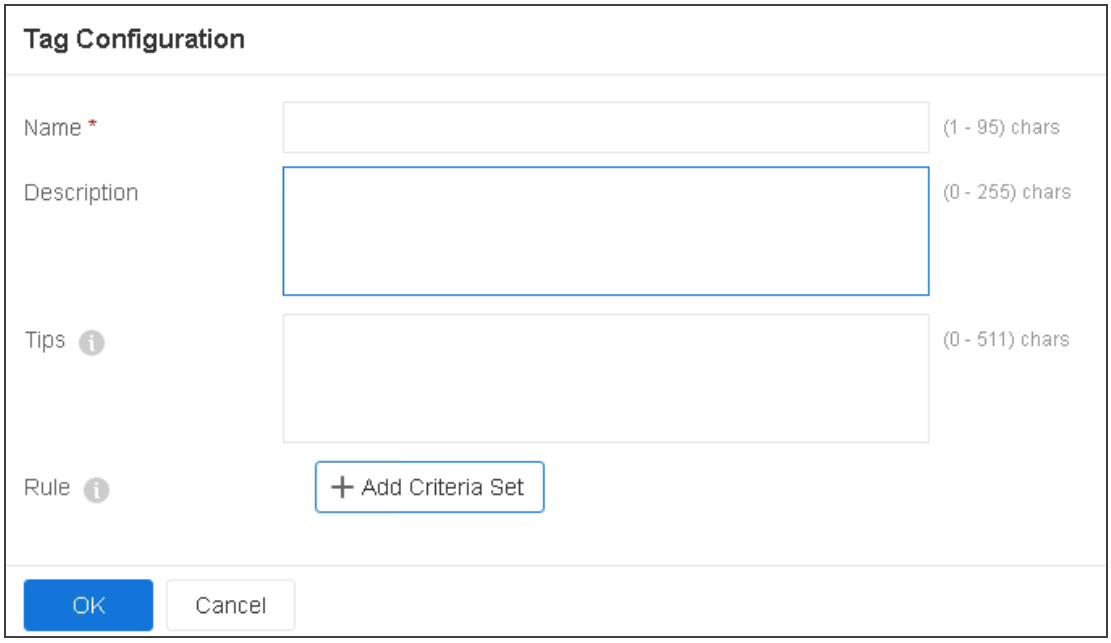
An endpoint tag is composed of one or more criteria sets, each consisting one or more conditions. Each endpoint tag can contain a maximum of 16 criteria sets and up to 16 conditions. The system supports to configure a maximum of 1,024 endpoint tags, with no more than 128 per VSYS.

- The logical relationship between criteria sets is "OR". If the endpoint information carried by a user matches one of the criteria sets within an endpoint tag, this endpoint tag is considered to be matched.
- The logical relationship between the conditions in a criteria set is "AND". The endpoint information carried by a user needs to match all conditions in a criteria set for it to be considered a match for that criteria set.

Configuring an Endpoint Tag

To configure an endpoint tag, take the following steps:

1. Select **ZTNA** > **Endpoint** > **Tag**.
2. Click **New**.



In the Tag Configuration tab, configure the corresponding options.

Option	Description
Name	Type the name of the endpoint tag. The length is 1 to 95 characters.
Description	Type description for the endpoint tag. The length is 1 to 255 characters.
Tips	Type the tip to be displayed on ZTNA Portal. The range is 0 to 511 characters. For application resources that an end user is not allowed to access because the endpoint device does not match an endpoint tag, configure a tip to let the end user know the

Option	Description
	reason and update the endpoint device to obtain the access privilege. URL addresses are supported in a tip. When it is displayed on the ZTNA portal, it will be presented as a hyperlink. By default, the tip for each endpoint tag is "Access Failed Contact your administrator". When a ZTNA policy binds multiple endpoint tags configured with tips: • If an end user matches any of the endpoint tags and is granted access to the application resource, no tip will be displayed for the corresponding application resource on the ZTNA portal. • If an end user is not granted access to the application resource because no endpoint tag is matched, all tips will be displayed for the corresponding application resource on the ZTNA portal. If all bound endpoint tags are not configured with tips, the default tip will be displayed.
Rule	Specify the criteria set and conditions. Each endpoint can contain up to 16 criteria sets and 16 conditions.
Add Criteria Set	Click **Add Criteria Set** to configure a criteria set and contained conditions for the endpoint tag. You can click the button to add more criteria sets.
Operating System	Select the operating system type. Windows, macOS, Linux, iOS, Android, and ChineseOS are supported.
Endpoint Type	Select the endpoint item name, including all supported predefined and custom endpoint items. Then, select the operator and value. You can click **New** to add more conditions; click **Delete** to delete

Option	Description
	a selected condition.

3. Click **OK** to save the configuration.
4. On the Tag page, you can view the configuration information of all endpoint tags and the number of times an endpoint tag is referenced by a ZTNA policy.
5. By clicking the value in the "References" column, you can view the ZTNA policies that are bound to this endpoint tag.
6. By clicking the ZTNA policy ID, you can view ZTNA policy configuration details.

Application Resource/Application Resource Group

Introduction

Application resource are used to define the applications, content, services, etc. that you want to access. You need to configure parameters such as address, protocol, and port number to specify an application resource entry. Application resource groups are used to define a group of application resources. The system supports to configure a maximum of 256 application resources and 64 application resource groups.

You can define an application resource entry in one of the following ways:

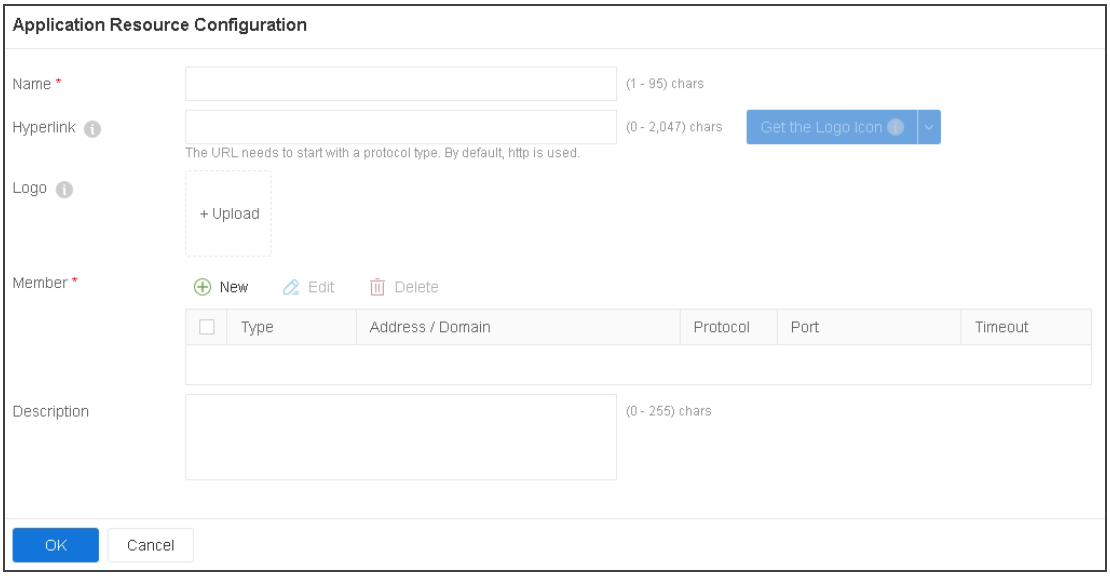
- Based on IP address, protocol, and port number
- Based on IP range, protocol, and port number
- Based on domain name, protocol, and port number

Configuring an Application Resource/Application Resource Group

To configure an application resource, take the following steps:

1. Select **Object** > **Application Resource Book** > **Application Resource**. Or select **ZTNA** > **Application Resource Book** > **Application Resource**.

2. Click **New**.



Option	Description
Name	Type the name of the application resource. The length is 1 to 95 characters.
Hyperlink	Type the hyperlink of the application resource. The length is 0 to 2047 characters. On the ZTNA portal displayed after a user logs in, the user can copy the hyperlink to access an application resource in a browser if the application resource is configured with an hyperlink; or, the user can directly click the application resource icon to access it (make sure the link work). An application resource without a hyperlink configured will not be displayed on the ZTNA portal. If the specified hyperlink does not contain the protocol type, the default HTTP protocol will be used.

Option	Description
	Get the Logo Icon: After a URL is configured, click this button. The system will automatically obtain the logo image corresponding to this URL. If no logo image can be obtained, the "The LOGO Icon is not found" prompt will appear. You can click to select a virtual router to which the URL belongs from the drop-down list.
Logo	Specifies the logo of the application resource, which is used to be displayed on the ZTNA Portal page. To do this, click **Upload** and select an authentication logo from your PC. The logo needs to be in the svg, ico, png, jpg, or jepg format, which cannot exceed 24 KB in size. Note: If you do not upload the logo of the application resource or automatically obtain the logo by configuring a URL, a default logo generated based on the first character of the application resource name is displayed in the application resource list and on the ZTNA Portal page.
Member	Click **New** to add a resource entry and configure the options. Each application resource can contain up to 16 entries. • Type: Specify the address type of the resource entry, including IPv4/Netmask, IPv6/Prefix, IPv4 Range and IPv6 Range and Domain. • Address: Specify the IP address or IP range of the resource entry.

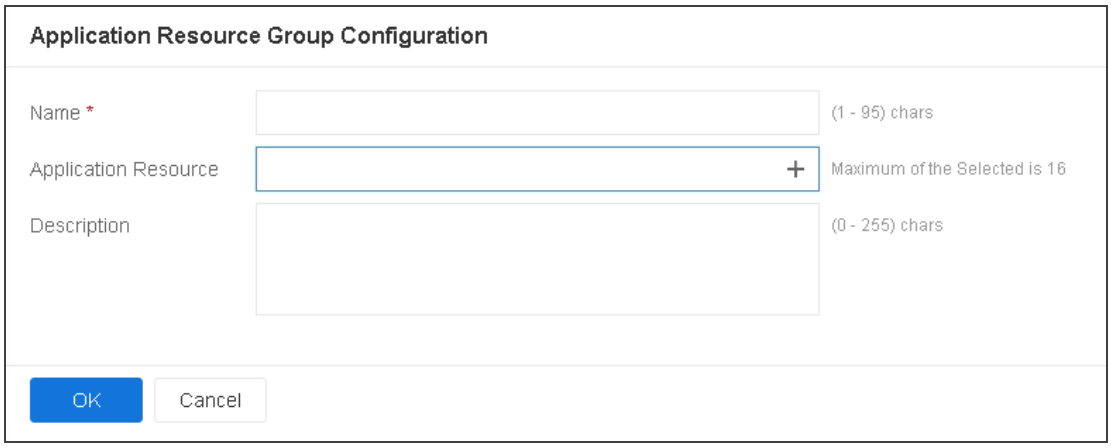
Option	Description
	• Protocol: Specify the protocol type of the resource entry. TCP and UDP are supported for application resources defined based on IP address. HTTP and HTTPS are supported for application resources defined based on domain name. • Port: Specify the port number or port range of the resource entry. If you specify a port number, the minimum port number and the maximum port number need to be the same. The value ranges from 1 to 65535. • Timeout: Specify the timeout value in seconds or days. The value range is 1 to 65535 when it is expressed in seconds and 1 to 1000 when in days. The default value is 1800s when the protocol is TCP, HTTP or HTTPS, and 60s when UDP.
Description	Type description for the application resource. The length is 0 to 255 characters.

3. Click **OK** to save the configuration.
4. On the Application Resource page, by clicking the "+" button in the list to unfold an application resource, you can view more details about it, including the group it belongs to and the ZTNA policy ID that is bound to it.

To configure an application resource group, take the following steps:

1. Select **Object** > **Application Resource Book** > **Application Resource Group**. Or select **ZTNA** > **Application Resource Book** > **Application Resource Group**.

2. Click **New**.



Option	Description
Name	Type the name of the application resource group. The length is 1 to 95 characters.
Application Resource	Select existing application resources. Or, click **New** to create an application resource. You can add up to 16 application resources.
Description	Type description for the application resource group. The length is 0 to 255 characters.

3. Click **OK** to save the configuration.

4. On the Application Resource Group page, by clicking the "+" button to unfold an application resource group, you can view more details about it, including the ZTNA policy ID that is bound to it.

ZTNA Policy

ZTNA grants access to users based on ZTNA policies. The system supports up to 2000 ZTNA policies. A ZTNA policy functions based on the matching condition and action. It supports the following dimensions as matching conditions:

- User/User group: When a user/user group matches the one configured in the ZTNA policy, this user/user group is considered to meet the matching condition.
- Endpoint tag: When the endpoint tag carried with an authenticated user matches the one configured in the ZTNA policy, this endpoint tag is considered to meet the matching condition.
- Application resource/Application resource group: When a requested application resource/application resource group matches the one configured in the ZTNA policy, this application resource/application resource group is considered to meet the matching condition.
- Schedule: When the user access time matches the one configured in the ZTNA policy, the access time is considered to meet the matching condition.

ZTNA policy can be configured with one or multiple matching conditions. For a ZTNA policy configured with multiple matching conditions, the policy is considered to be hit and the traffic will be processed based on the action specified in the policy only when all matching conditions are met. When a matching condition is not configured in a ZTNA policy, all objects are considered to meet this matching condition. The policy action includes two types (at least one must be configured):

- permit: User traffic hitting a specified ZTNA policy will be granted access to resources configured in the policy.
- deny: User traffic hitting a specified ZTNA policy will be denied access to resources configured in the policy.

User traffic that does not hit any ZTNA policies will hit the ZTNA default policy and be processed based on the default action.

Description about ZTNA Policy Matching

For Internet access scenarios, the following traffic will experience ZTNA policy matching, while other traffic will experience firewall security policy matching:

- Traffic that enters from a ZTNA tunnel interface, and the zone service type of the traffic's egress interface, as found based on the route, is not a WAN zone.

For intranet access scenarios, if the traffic meets any of the following conditions, ZTNA policy matching is performed, and firewall security policy matching is performed for other traffic:

- The zone service type of the traffic's ingress interface is a ZTNA zone, and the zone service type of the traffic's egress interface, as found based on the route, is not a WAN zone.
- The zone service type of the traffic's egress interface, as found based on the route, is a ZTNA zone.

For more information about how to configure a zone service type, see Specifying the Service Type of Zone.

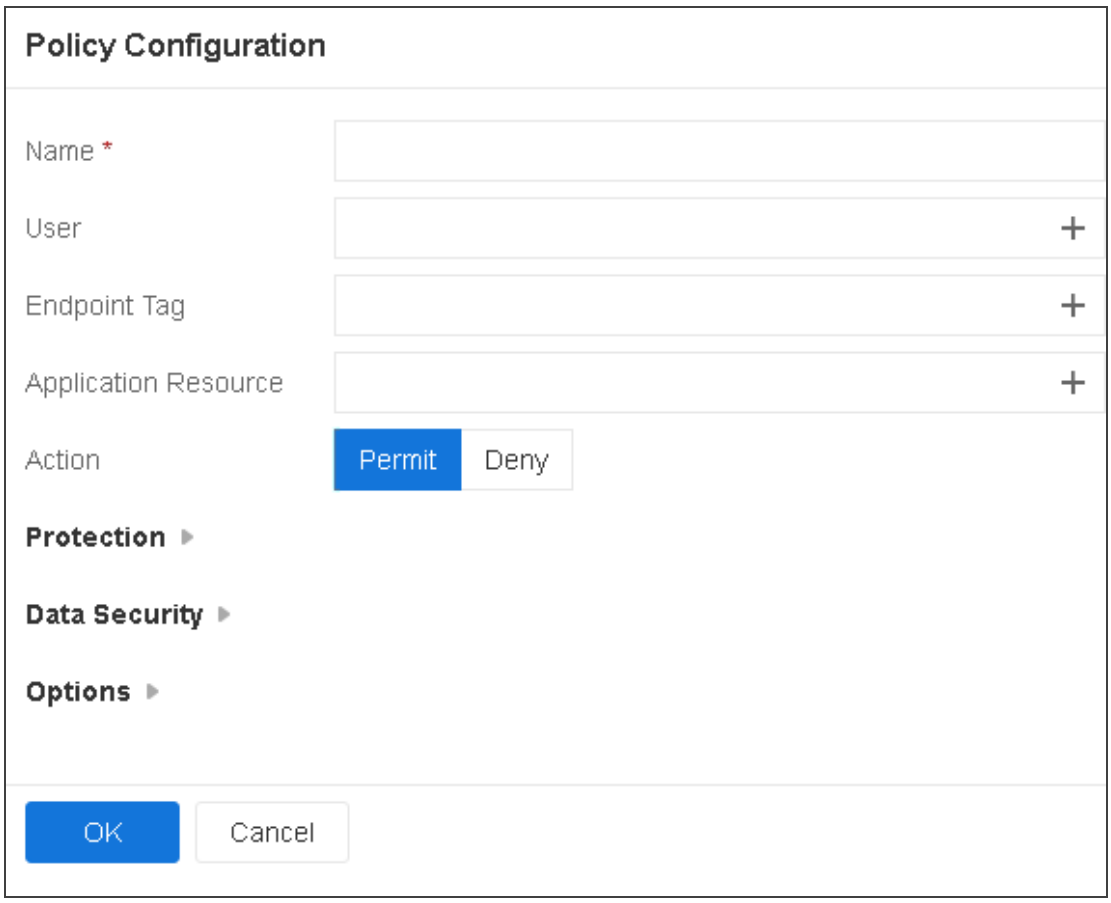
Configuring ZTNA Policy

Before you start

- Read "ZTNA Policy" on Page 790.

To configure a ZTNA policy, take the following steps:

1. Select **ZTNA** > **Policy**.
2. Click **New**.



In the Policy Configuration tab, configure the corresponding options.

Option	Description
Name	Type the name of the ZTNA policy. The length is 1 to 95 char-

Option	Description
	acters.
User	Select the user/user group to be bound. • AAA Server: Specifies the AAA server that a user/user group belongs to. Select an existing AAA server from the drop-down list. Or, click **New** to create a AAA server. For information about AAA server configuration, refer to Configuring AAA. • Select User/Select User Group: Select existing users/user groups. Or, click **New** to create a user/user group. • Input User/User Group: Type the user name/user group name, and then click **Add**. The user name length is 1 to 63 characters. The user group name length is 1 to 127 characters. At most 8 users and 8 user groups can be added.
Endpoint Tag	Select the endpoint tags to be bound. You can select from existing endpoint tags. Or, click **New** to create one. For information about endpoint tag configurations, see Configuring Endpoint Tags. Each policy can be bound with 10 endpoint tags.
Application Resource	Select the application resources/application resource groups to be bound. You can select from existing application resources and application resource groups. Or, click **New** to create one. For information about application resource/application resource group configurations, see Configuring Application Resource/Application Resource Group. Each policy can be bound with 10 application

Option	Description
	resources and 10 application resource groups.
Action	Select the action to be performed on user traffic hitting the policy, i.e. permitting or denying access to the bound application resources.

Click Threat Prevention to add threat prevention configurations

Option	Description
Anti-Virus	When the system is installed with the anti-virus license, click to enable the anti-virus function and bind an anti-virus profile to a ZTNA policy to achieve virus detection on traffic matching the ZTNA policy and process the detected viruses based on the Anti-Virus Profile. For information about file filter, please refer to Anti Virus.
Sandbox	When the system is installed with the sandbox license, click to enable the sandbox function and bind a sandbox profiles to a ZTNA policy to achieve sandbox detection on traffic matching the ZTNA policy. By using the cloud sandbox and the local sandbox technology, the system analyzes the suspicious file and collects the actions of the suspicious file, verifies the legality of the file, gives the analysis result to the system and deals with the malicious file based on the actions set by system. For information about file filter, please refer to Sandbox.
IPS	When the system is installed with the IPS license, click to enable the IPS function and bind an IPS profile to a ZTNA policy to detect network attacks in traffic matching the ZTNA policy and perform actions such as blocking on the attacks based on the IPS Profile. For

Option	Description
	information about file filter, please refer to Intrusion Prevention System.

Click Data Security to add data security configurations

Option	Description
File Filter	Click to enable the file filter function and bind a file filter profile to the ZTNA policy so as to perform file detection on traffic matching the ZTNA policy and perform control actions on the file matching the filter conditions based on the file filter profile. For information about file filter, please refer to File Filter.
File Content Filter	Click to enable the file content filter function and bind a file content filter profile to the ZTNA policy so as to perform file content detection on traffic matching the ZTNA policy and perform control actions such as blocking or logging based on the file content filter profile. For information about file filter, please refer to File Content Filter.

Click Options to configure advanced policy configurations.

Option	Description
Schedule	Specify the schedules to be matched. You can select from existing ones. Or, click **New** to create a schedule. For information about schedule configurations, see Creating a Schedule. Each policy can be configured with up to 10 schedules.
Log	You can log ZTNA policy matching in the system logs as required. Multiple options are available. • Deny: Generates logs when the traffic matching the policy

Option	Description
	is denied. • Session start: Generates logs when the traffic matching the policy starts its session. • Session end: Generates logs when the traffic matching the policy ends its session.
Position	Select a policy position from the **Position** drop-down list. Each ZTNA policy is labeled with a unique ID or name. When ZTNA traffic flows into a device, the device will query for the policy rules by turn, and processes the traffic according to the first matched rule. However, the policy ID is not related to the matching sequence during the query. The sequence displayed in ZTNA policy list is the query sequence for policy rules. The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name. The default position is the bottom.
Description	Type description for the policy. The length is 0 to 255 characters.

3. Click **OK** to save the configuration.

4. On the Policy page, you can view the configuration information of all policies and manage policy configurations.

   Manage policy configurations on the Policy page

Option	Description
Filter	Select filter conditions from the drop-down list. The policy table will display the policies matching the filter conditions.

Option	Description
Edit	Select a policy and click **Edit** to change the policy configuration.
Delete	Select a policy and click **Delete** to delete the selected policy.
Copy, Paste	Select a policy, click **Copy** and then **Paste**. Select the position from the drop-down list to add a policy with the same configuration and place it at the specified position.
Move	Select a policy, click **Move** and select the position from the drop-down list to change the policy position.

Click " ⋮ " and select an option.

Option	Description
Enable	Select a disabled policy and click **Enable** to enable it.
Disable	Select an enabled policy and click **Disable** to disable it.
Default Policy Action	Specify the action to be performed on user traffic that does not hit any ZTNA policies. Select this option. Then, in the displayed dialog box, you can view default policy statistics and configure the following options: • Default Action: Permit or deny access. • Log: Click this button to enable logging of traffic hitting the default policy.
Clearing Policy Hit Count	Select this option. In the displayed dialog box, you can clear corresponding policy statistics by selecting "All Policies", "Default Policy" or specifying the policy ID or name.

Address Pool

Introduction

The servers allocate IP addresses in the address pools to the clients. After the client connects to the server successfully, the server will fetch an IP address along with other related parameters (e.g., DNS server address and WIN server address) from the address pool and then allocate the IP address and parameters to the client.

You can create and execute an IP binding rule to meet the fixed IP requirement. The IP binding rule includes the IP-user binding rule and the IP-role binding rule. The IP-user binding rule binds the client to a fixed IP address in the configured address pool. When the client connects to the server successfully, the server will allocate the binding IP address to the client. The IP-role binding rule binds the role to an IP range in the configured address pool. When the client connects to the server successfully, the server will select an IP address from the IP range and allocate the IP address to the client.

After the client successfully connects to the server, the server will check the binding rules in a certain order to determine which IP address to allocate. The order is shown as below:

- Check whether the IP-user binding rule is configured for the client. If yes, allocate the bound IP address to the client; if no, the server will select an IP address which is not bound or used from the address pool, then allocate it to the client.
- Check whether the IP-role binding rule is configured for the client. If yes, get an IP address from the IP range and allocate to the client; if no, the server will select an IP address which is not bound or used from the address pool, then allocate it to the client.



Notes: IP addresses in the IP-user binding rule and the IP address in the IP-role binding rules should not overlap.

Configuring an Address Pool

To configure an address pool, take the following steps:

1. Select **Object > Access Address Pool**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.
3. Click **New**.

In the Access Address Pool Configuration tab, configure the following options.

Option	Description
Access Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved start IP	Specifies the reserved start IP of the address pool.
Reserved end IP	Specifies the reserved end IP of the address pool.
Netmask	Specifies the netmask in the dotted decimal format.
Prefix Length	Specifies the prefix for this IPv6 address range. The range is 111 to 128.
DNS1/2/3/4	Specifies the DNS server IP address for the address pool. It is optional. 4 DNS servers can be configured for one address pool at most.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to 2 WIN servers can be configured for one address pool. This option can only be configured when the created IPv4 address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the **User** box.
IP	Type the IP address into the **IP** box.
New	Click **New** to add an IP user binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Type the role name into the **Role** box.
Start IP	Type the start IP address into the **Start IP** box.
End IP	Type the end IP address into the **End IP** box.
New	Click **New**to add an IP role binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.
Up/Down/Top/Bottom	System will query IP role binding rules by turn, and allocate the IP address according to the first matched rule. You can move the location up or down at your own choice to adjust the matching sequence accordingly.

4. Click **OK** to save the settings.

When a user name is binding with multiple roles corresponding to IP role binding rules, the system will query IP role binding rules by turn, and allocate the IP address according to the first matched rule. To adjust the sequence of IP role binding rules, in the Access Address Pool page,

select an address pool and click **Move IP-Role Binding**. In the **Move IP-Role Binding** dialog box, select the role to be adjusted and then click **Up/Down/Top/Bottom**.

Single Packet Authorization (SPA)

Introduction

Single Packet Authorization (SPA) is a universal access technology concept. Its main purpose is to hide the host's port number and therefore the service running on it will be hidden. The system will open the port only for packets carrying expected information.

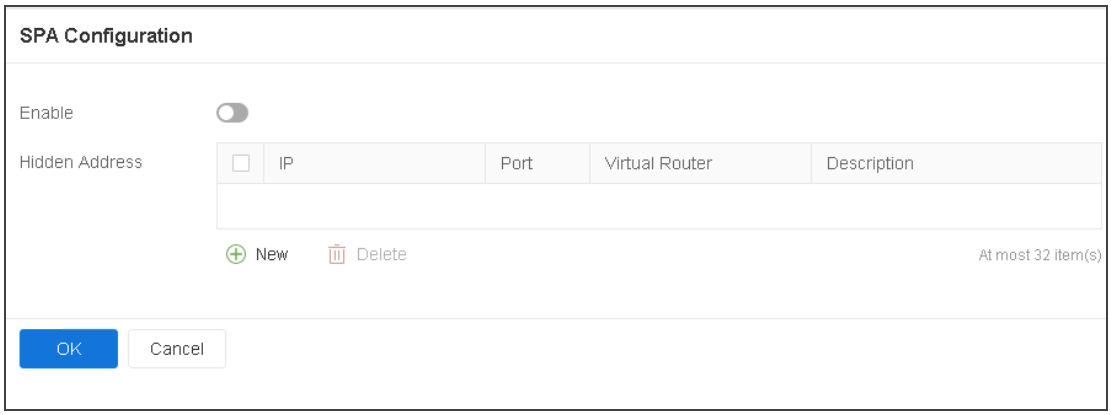
The ZTNA device supports enabling the SPA function and hiding the ZTNA service IP address and port number. ZTNA client also needs to enable the SPA function and pass the authorization before establishing a connection to the device. After SPA is configured, the SPA process for ZTNA users logging in through the client is as follows:

1. ZTNA client sends knock packets to ZTNA device with the knock port number being the destination port number.
2. ZTNA device checks the destination IP address of the knock packets. If the destination IP address is not a configured hidden IP address, it will be discarded. If it is a configured hidden IP address, ZTNA device will verify it and generate a permit entry with the destination IP address, destination port number and source IP address.
3. ZTNA client sends a connection request.
4. ZTNA device checks the requested IP address and port number. If they are hidden IP address and port number, ZTNA device will search for the matched permit entry. If a matched permit entry is found, the connection request is accepted. Otherwise, the request will be discarded.

Configuring Single Packet Authorization (SPA)

To configure SPA for ZTNA, take the following steps:

1. Select **ZTNA** > **SPA** > **SPA Configuration**.



Option	Description
Enable	Click to enable the SPA function. By default, it is disabled.
Port	Specifies the local knock port where the ZTNA device listens for knock packets. The range is 1025 to 65535. The default knock port is 60001.
Hidden Address	Click **New** to add the hidden addresses. • IP: Specifies the IPv4 address to be hidden, i.e. the IPv4 address of the egress interface configured in Interface. • Port: Specifies the port number to be hidden, i.e. the service port configured in Interface. The range is 1 to 65535. • Virtual Router: Specifies the virtual router that the interface of the hidden IP address belongs to. • Description: Specifies the description. The range is 0 to 63 characters.

2. Click **OK** to save the configuration.

To view the SPA permit entries that the ZTNA device generates, select **ZTNA** > **SPA** > **SPA List**.

- Client IP: indicates the source IP address of the client.
- Service IP: indicates the hidden IP address, which is also the destination IP address.
- Virtual Router: indicates the virtual router that the interface of the hidden IP address belongs to.
- Port: indicates the hidden port number, which is also the destination port number.
- Life time (seconds): indicates the lifetime of the permit entry. After the lifetime elapses, the permit entry will be deleted.

Secure Connect Client Management

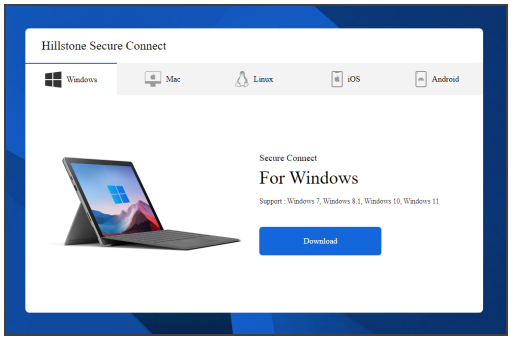
End users can download Secure Connect clients at the following addresses:

- Client download address on the device: https://IP-Address:Port-Number. The "IP-Address" and "Port-Number" refer to the IP address of the egress interface and HTTPS port number specified in the configuration of the SSL VPN or ZTNA instance.
- Client download address provided by Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.

By default, the two addresses use the same download source, and the downloaded Secure Connect client is also the same.

Customizing Secure Connect Download Page

You can customize the title and background of the download address on the device. The default download page is shown as below:



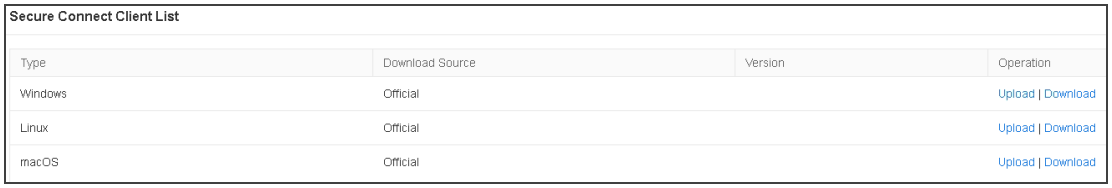
To customize the Secure Connect download page, take the following steps:

1. Select **System > Secure Connect Client Management**.
2. In the "Configure Secure Connect Client Download Page" area, click **Upload Background Picture > Browse** to select the background picture. The picture needs to be PNG format. The recommended resolution is 1920px*1080px. The size cannot exceed 2MB.
3. Click **Upload** to upload the background picture to system. After uploading successfully, you will have completed the background picture modification.
4. Enter the title in the **Download Page Tittle** box to customize the title of the download page. The length is 1 to 63 characters.
5. Click **OK** to save the settings. Clicking **Cancel** will only affect the authentication page title modification.

If you want to restore the default picture, click **Restore Default Background** . Then click **OK**.

Customizing Client Download Source

By default, the client download source on the device is the same with that on Hillstone Networks Official Website. In the application scenario where you want end users to download and use specific Secure Connect clients, such as a client of the specified version or a customized client, you can import the client into the system to overwrite the default download source on the device. You can import Windows, macOS and Linux type clients.



To import the client, take the following steps:

1. Select **System > Secure Connect Client Management**.
2. In the "Secure Connect Client List" area, locate the type of client to be imported and click **Upload**.
3. In the "Upload Secure Connect Client for Windows/macOS/Linux" dialog box, click **Browse** and select the client file to be imported, and click **Upload**. The file name should be in the "xxx_version_check.exe/run/dmg/pkg" format. "xxx" indicates the file name; "version"indicates the client version, starting with the letter "v"; "exe" is the extension for Windows type client file; "run" is the extension for Linux type client file; "dmg" and "pkg" are the extensions for macOS type client file. The file size cannot exceed 100MB. An example is "secure-connect_v1.4.9.2000_1a6755fe.exe".
4. After uploading, the download source for this client will change from "Offical" to "Local" in the "Secure Connect Client List".
5. Click **Download** to check the downloaded client is the imported one.
6. Click **Delete** to delete the imported client. After the imported client is deleted, the download source will be resorted to "Official".

ZTNA Portal

After a ZTNA user logs in, the user terminal will be prompted with the ZTNA portal page via the default browser, displaying the applications resources to which the user is granted access and not granted access.

- When the user's authentication information and endpoint tag match the ZTNA policy whose action is Permit, the user is granted access to the application resources bound with this policy.
- When the user's authentication information matches teh ZTNA policy but the endpoint tag does not match the ZTNA policy, the user is not granted access to the application resource bound with this policy.

For an application resource to which a user is granted access, the user can click the application resource icon on the ZTNA Portal page to switch to the desired URL address. Or, the user can copy the URL address to a browser to access the application resource. For an application resource to which a user is not granted access, the user can view the reason.

The ZTNA portal page does not display the following application resources:

- Application resources that the user is not allowed to access
- Application resources that the user is allowed to access, but no hyperlink is specified when the application resource is defined

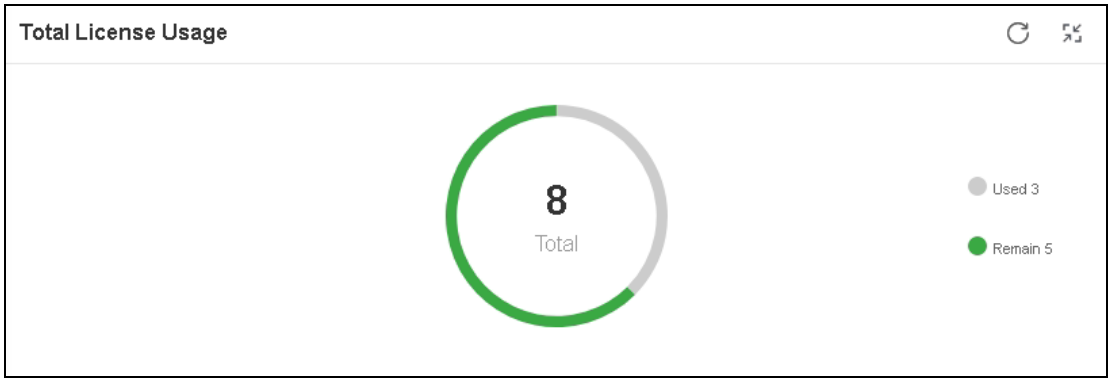
After the ZTNA Portal page is closed, the user can select "Application Resource List" from the ZTNA client menu to obtain the ZTNA Portal page again.

Monitor

Select **ZTNA** > **Monitor** > **Summary** to enter the ZTNA monitor page.

ZTNA License Usage

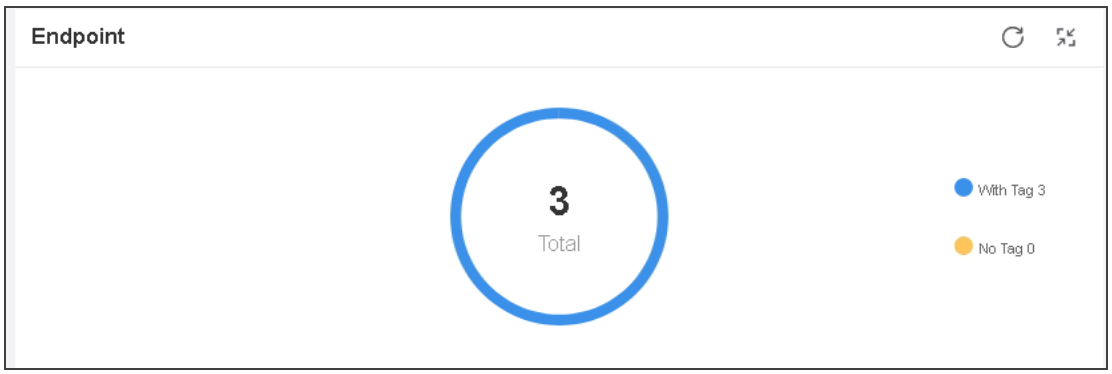
Click the refresh icon to obtain real-time ZTNA license usage.



- In the root VSYS mode, you can view the total ZTNA capacity, the number of used ZTNA licenses and the number of available ZTNA licenses. The number of used ZNTA licenses include all that are used by ZTNA and SSL VPN users.
- In the non-root VSYS mode, you can view the total number of ZTNA licenses that can be shared by all VSYS and the total number of ZTNA licenses that are used by all VSYS.

Online Endpoint Statistics

After a ZTNA user logs in, the system will collect user endpoint information periodically and generate endpoint tags for the user based on endpoint tag criteria. A user endpoint can hit multiple or zero endpoint tags. The number of online endpoints include both the endpoints hitting one or more endpoint tags and the endpoints that do not hit any endpoint tags.



Click the refresh icon to obtain real-time statistics of online endpoints.

Endpoint Hit Top 10

An endpoint tag can be hit multiple times or is not hit. Endpoint Hit Top 10 displays the names of the endpoint tags with top 10 hit counts in descending order since system startup.

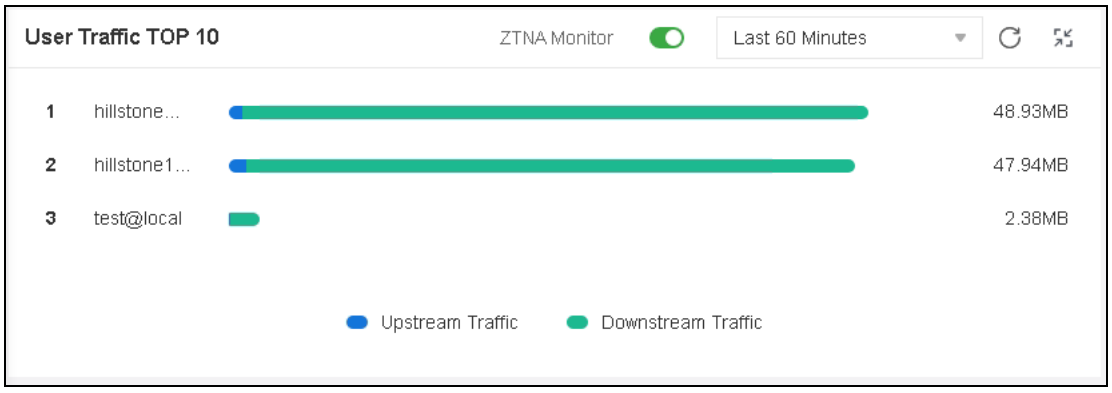


Click the refresh icon to obtain real-time ranking of top 10 endpoint tag hits.

User Traffic Top 10

User traffic refers to data interaction generated with application resource access, including the total traffic, upstream traffic and downstream traffic. To view user traffic top 10 statistics, make sure the ZTNA monitor function is enabled.

You can view top 10 real-time ZTNA user traffic statistics as well as the ranking for the latest 1 hour, 1 day and 1 month.



Click **Upstream Traffic** or **Downstream Traffic**. When the Upstream Traffic icon turns gray, you can view the top 10 downstream traffic users. When the Downstream Traffic icon turns gray, you

can view the top 10 upstream traffic users. By default, the ranking for the total traffic users is displayed.

Click the refresh icon to obtain real-time ranking.

Note: This function relies on the statistics set configuration of the monitor function. To view ZTNA user traffic top 10, make sure "User monitor" is enabled and the "Bandwidth" option for "User/IP Statistics" is selected on the **Monitor** > **Monitor Configuration** page.

Viewing and Managing Online Users

To manage and view the status information of all ZTNA online users, take the following steps:

1. Select **ZTNA** > **Monitor** > **User Status**.

    a. Login Time: indicates the login time of the online user;

    b. User Name: indicates the user name of the online user;

    c. AAA Server: indicates the AAA server name to which the online user belongs;

    d. ZTNA Server: indicates the ZTNA service name that the online user accesses;

    e. User IP: indicates the IP address of the online user that the ZTNA server assigns;

    f. Endpoint Name: indicates the user endpoint name;

    g. Endpoint IP: indicates the user endpoint IP address, i.e. the public IP address of the user;

    h. OS: indicates the operating system of the user endpoint;

    i. Endpoint Tag: indicates the endpoint tag associated with the online user;

    j. Allowed Application Resources: indicates the application resources that the online user is granted access;

k. Denied Application Resources: indicates the application resources that the online user is not granted access;

l. Upstream Speed: indicates the upstream speed of the online user;

m. Downstream Speed: indicates the downstream speed of the online user.

2. Click **Filter** to add filter conditions to view the detailed information of ZTNA online users that meet the filter conditions.

3. By selecting one or more users and clicking **Force Log Off**, you can force disconnecting a user with the ZTNA server.

Note: To view upstream and downstream speed statistics, make sure the ZTNA monitor function is enabled.

Endpoint Tag Log

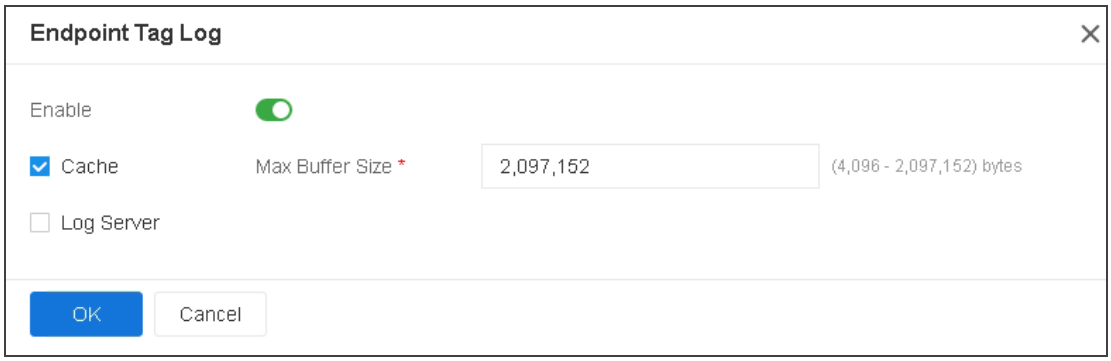
The system support management of endpoint tag logs by using the endpoint tag log function. To configure and manage endpoint tag logs, take the following steps:

1. Select **Monitor** > **Log** > **Endpoint Tag Log** or select **ZTNA** > **Endpoint Tag Log**.

   - Time: indicates the endpoint tag log's generation time.
   - Type: indicates the endpoint tag log type, including login, logout, abnormal logout, endpoint tag update and application resource update.
   - User Name: indicates the user name.
   - User IP: indicates the user IP address.
   - AAA Server: indicates the AAA server to which the user belongs.
   - Endpoint Name: indicates the endpoint name.
   - Endpoint IP: indicates the endpoint IP address.

- OS: indicates the operating system of the endpoint.
- Endpoint Tags: indicates the endpoint tag associated with the user.
- ZTNA Server: indicates the ZTNA service name that the user accesses.
- Allowed Application Resources: indicates the application resources that the user are allowed to access.
- Denied Application Resources: indicates the application resources that the user are not allowed to access.

2. Click **Configure** and enter the **Endpoint Tag Log** page.



Option	Description
Enable	Click the button to enable the endpoint tag log function and select the destinations where the endpoint tag logs will be sent to. You can select multiple destinations. By default, the endpoint tag log function is enabled and the logs will be sent to the memory buffer.
Cache	Select the check box to send endpoint tag logs to the memory buffer.
Max Buffer Size	When configuring the system to send endpoint tag logs to the

Option	Description
	memory buffer, you can define the memory buffer size for storing the endpoint tag logs. The range is 4096 to 2097152, in bytes. The default value is 2097152.
Log Server	Select the check box to send endpoint tag logs to the syslog server, in plaintext. You need to configure a syslog server first. Click the "" link to view all syslog servers that have been configured. For configuration information about syslog server, refer to Creating a Log Server.

3. Click **Filter** to view endpoint tag logs that match the specified filtering conditions.
4. Click **Clear** to clear all endpoint tag logs.

   Note: This option is not supported for devices that support sending log information to the local database.
5. Click **Export** to export all endpoint tag logs to a local file.

Chapter 10 Object

This chapter describes the concept and configuration of objects that will be referenced by other modules in system, including:

- "Address" on Page 814: Contains address information, and can be used by multiple modules, such as policy rules, NAT rules, QoS, session limit rules, etc.
- "Host Book" on Page 831: A collection of one domain name or several domain names.
- "Service Book" on Page 838: Contains service information, and can be used by multiple modules, such as policy rules, NAT rules, QoS, etc.
- "Application Book" on Page 851: Contains application information, and it can be used by multiple modules, such as policy rules, NAT rules, QoS, etc.
- "SLB Server Pool " on Page 904: Describes SLB server configurations.
- "Schedule" on Page 910: Specifies a time range or period. The functions (such as policy rules, QoS rules, host blacklist, connections between the PPPoE interface and Internet) that use the schedule will take effect in the time range or period specified by the schedule.
- "AAA Server" on Page 912: Describes how to configure an AAA server.
- "User" on Page 955: Contains information about the functions and services provided by a Hillstone device, and users authenticated and managed by the device.
- "Role" on Page 976: Contains role information that associates users to privileges. In function configurations, different roles are assigned with different services. Therefore, the mapped users can gain the corresponding services as well.
- "Track Object" on Page 985: Tracks if the specified object (IP address or host) is reachable or if the specified interface is connected. This function is designed to track HA and interfaces.

- " URL Filtering" on Page 992: URL filter controls the access to some certain websites and records log messages for the access actions.
- "NetFlow" on Page 1624 : Collect the user's incoming traffic information according to the NetFlow profile, and send it to the server with NetFlow data analysis tool. For more information, see **Monitor** > "NetFlow" on Page 1624.
- "End Point Protection" on Page 1452: Obtain the endpoint data monitored by the endpoint security control center by interacting with it, and then specify the corresponding processing action according to the security status of endpoint, so as to control the endpoint network behavior.
- "IoT Monitor" on Page 1460: Identify the network video monitoring devices, like IPC (IP Camera) and NVR (Network Video Recorder) via the flowing traffic, then monitor the identified devices and block illegal behaviors according to the configurations.

Address

IP address is an important element for the configurations of multiple modules, such as policy rules, NAT rules and session limit rules. Therefore, system uses an address book to facilitate IP address reference and flexible configuration. You can specify a name for an IP range, and only the name is referenced during configuration. The address book is the database in system that is used to store the mappings between IP ranges and the corresponding names. The mapping entry between an IP address and its name in the address book is known as an address entry.

System provides a global address book. You need to specify an address entry for the global address book. When specifying the address entry, you can replace the IP range with a DNS name. When you configure NAT, the system will use interfaces of the configured IP addresses as address entries and add them to the address book automatically. Furthermore, an address entry also has the following features:

- All address books contain the following default address entries named **Any**, **IPv6-Any** and **private_network**. The IP address of **Any** is 0.0.0.0/0, which is any IPv4 address. The IP

address of **IPv6-Any** is ::/0, which is any IPv6 address. The IP addresses of **private_network** are 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, that all private network address. **Any**, **IPv6-Any** and **private_network** can neither be edited nor deleted .

- One address entry can contain another address entry in the address book.
- If the IP range of an address entry changes, StoneOS will update other modules that reference the address entry automatically.

Address book supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry.

Global Configuration of Address Book

The global configuration of the address book is used to enable or disable the ordered address book function. In the ordered address book, the address members can be stored in the configured sequence of IP addresses. In some specific business scenarios, when there are multiple IP addresses that need to be NATed, the administrator requires a one-to-one mapping of IP addresses, traditionally achieved by creating multiple NAT rules and individually translate each IP address. To enhance the O&M efficiency, you can directly reference the ordered address book in NAT rules, allowing multiple IP addresses within a single NAT rule to be translated one-to-one based on the specified order of IP address. Referencing the ordered address book in NAT rules not only improves the execution efficiency and accuracy of NAT rules but also enables you to modify a single NAT rule when changing the business, reducing maintenance complexity.

Enabling Ordered Address Book Function

By default, the Ordered Address Book function is disabled. To enable the ordered address book function, take the following steps:

1. Select **Object** > **Address Book**.
2. Click **Global Configuration**. In the **Address Book Global Configuration** panel, click **Enable** next to **Ordered Address Book**. This way, you can add ordered address members when

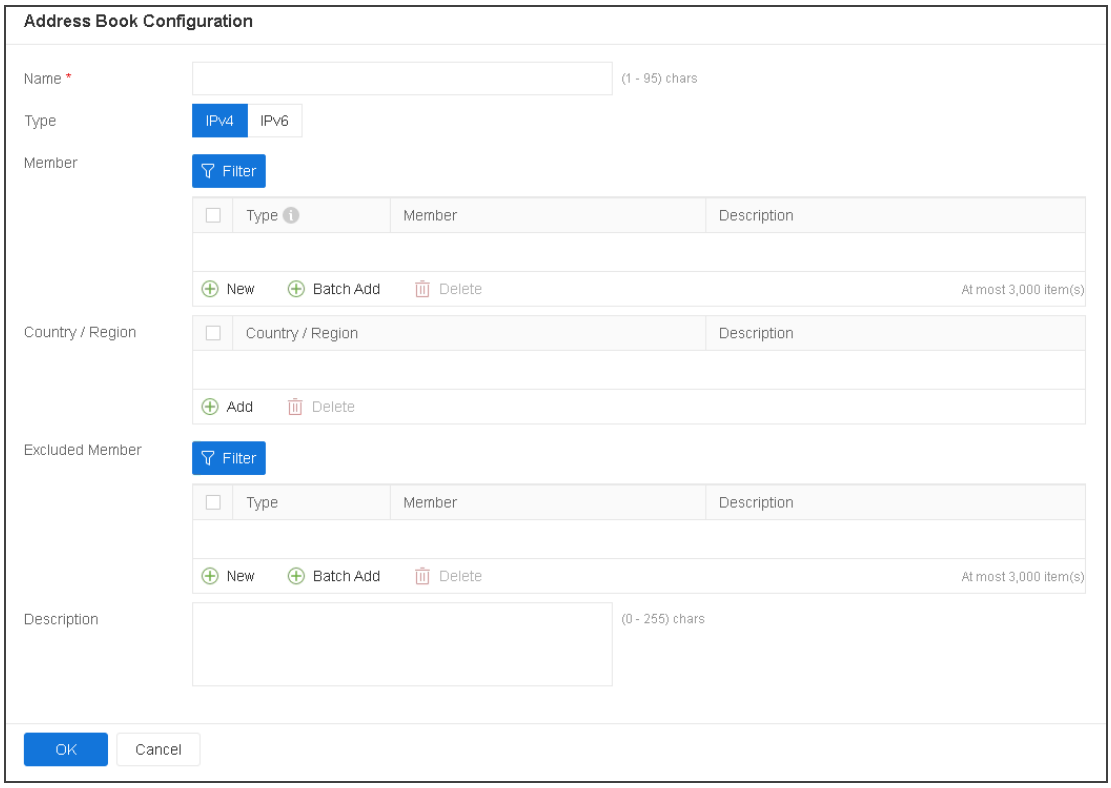
creating an address book and the system will save them in the configured order of these address members. For more information, see Creating an Address Book.

Notes: When the current address book contains the configuration of ordered address book, you cannot disable the Ordered Address Book function. To disable this function, delete the ordered address book configured in the system first.

Creating an Address Book

To create an address book, take the following steps:

1. Click **Object>Address Book**.
2. Click **New**.



Basic	
Name	Type the address book name into the Name box.
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type.
Description	Enter a description for the address book.
Ordered member address	Turn on the switch to configure ordered address members of the ordered address book. Once enabled, the enabled status cannot be changed. To configure this option, you need to enable the Ordered Address Book function in the global configuration of address book.
Ordered Address Members	Configure the ordered address members of the ordered address book, including creating, deleting, or moving an ordered address member. • Creating an ordered address member: click **New**. In the field in the Member column, enter an IPv4 or IPv6 address. In the field in the Description column, enter a description for the ordered address member. • Deleting an ordered address member: select an ordered address member and click **Delete** to delete it. • Moving an ordered address member: select an ordered address member, click **Move**, and then select **Move Top**, **Move Bottom**, or **To Line**. If you select **To Line**, you need to enter the line number in the field.
Member	

Basic	

Member	Configure the address member.
	• If the **Type** parameter is set to IPv4:
	  • Click **New**. You can add an address member of the IP/Netmask, IP Range, Hostname, Address Book, or IP/Wildcard type as needed. To do this, select a member type from the Type drop-down list, enter or select the corresponding configuration in the Member field, and then enter a description for this address member in the **Description** field.
	  • Click **Batch Add**. In the **Add Addresses** panel, you can add address members in batches.
	  In the **IP Address** text box, configure an IP/netmask, IP range, or IP/wildcard and its description in each line and press Enter. Use a semicolon (;) to separate the address and its description;
	  Select a VRouter to which the address members belong from the Hostname drop-down list. In the text box below, configure a hostname and its description in each line and press Enter. Use a semicolon (;) to separate the hostname and its description;
	  Select one or more address books from the **Address Book** drop-down list.

Basic	

	• Click . From the **Type** or **Member** drop-down list, filter address members by type or content.
	• If the **Type** parameter is set to IPv6:
	  • Click **New**. You can add an address member of the IPv6/Prefix, IPv6 Range, Hostname, Address Book, or IPv6/Wildcard type as needed. To do this, select a member type from the Type drop-down list, enter or select the corresponding configuration in the Member field, and then enter a description for this address member in the **Description** field.
	  • Click **Batch Add**. In the **Add Addresses** panel, you can add address members in batches.
	In the **IPv6 Address** text box, configure an IPv6/prefix, IPv6 range, or IPv6/wildcard and its description in each line and press Enter. Use a semicolon (;) to separate the address and its description;
	Select a VRouter to which the address members belong from the Hostname drop-down list. In the text box below, configure a hostname and its description in each line and press Enter. Use a semicolon (;) to separate the hostname and its

Basic	
	description; Select one or more address books from the **Address Book** drop-down list. • Click . From the **Type** or **Member** drop-down list, filter address members by type or content. Note: • When you add the IP/Wildcard member, binary 1 indicates exact match and 0 indicates fuzzy match in wildcard netmask. The subnet mask format can not be configured. Meanwhile, the address book with the IP/Wildcard member cannot be referenced by QoS policy. • In the IP geography database supported by StoneOS 5.5R10F2 and later F versions, StoneOS 5.5R11 and later, the territorial information of IP addresses within China is annotated at the provincial and city levels. In addition, Hong Kong S.A.R. (China), Macao S.A.R. (China), and Taiwan (China) are adjusted to provinces of China. After you upgrade the device system (authorized by the license outside China) to a version above, the existing address book configurations of Hong Kong S.A.R. (China), Macao S.A.R. (China), and Taiwan (China) are automatically deleted.

Basic	
	• When the type of the address entry member is IPv6/Wildcard, the 128bit wildcard mask must consist of consecutive 8 (or integer multiples of 8) zeros or consecutive 8 (or integer multiples of 8) 1s, such as FF00::FFFF. • A maximum of 8 address members of the IP/Wildcard type or the IPv6/Wildcard type are allowed to be configured in each address book entry. • Only the security policy and the IPv6 address book support the address entry with the IPv6/Wildcard member added.
Delete	Delete the selected member from the list.
Country/Region	
Country/Region	Specifies the country or region for the address member, and the Country/Region parameter is available only in the IPv4 address book. Click "Add" . In the **Country/Region** dialog box, add an address member of the Country/Region type as needed. After you select a country/region, this country/region is displayed in the **Country/Region** dialog box. If you select CN China, you can click "+" in front of CN China to select the corresponding province and city. **Note**: Province and city are not available in the version controlled by the license outside China.

Basic	
	• The address book with the Country/Region member can only be referenced by the security policy, policy-based route rules, and PTF dynamic IP blacklist. • The address book with the Country/Region member cannot be configured with the **Excluded Member** settings.
Description	Configure the description field for the country/region.
Excluded Member	

Member	Configure the excluded address member.
	• If the **Type** parameter is set to IPv4:
	  • Click **New**. You can add an excluded member of the IP/Netmask or IP Range type as needed. To do this, select a member type from the Type drop-down list, enter or select the corresponding configuration in the Member field, and then enter a description for this address member in the **Description** field.
	  • Click **Batch Add**. In the **Add Excluded Addresses** panel, you can add excluded address members in batches.
	  In the **IP Address** text box, configure an IP/netmask or IP range and its description in each line and press Enter. Use a semicolon (;) to separate the address and its description;

Basic	

	• Click next to the table header **Type** or **Member** to filter excluded address members by type or content.
	• If the **Type** parameter is set to IPv6:
	  • Click **New**. You can add an excluded member of the IPv6/Prefix or IPv6 Range type as needed. To do this, select a member type from the Type drop-down list, enter or select the corresponding configuration in the Member field, and then enter a description for this address member in the **Description** field.
	  • Click **Batch Add**. In the **Add Excluded Addresses** panel, you can add excluded address members in batches.
	  In the **IPv6 Address** text box, configure an IPv6/prefix or IPv6 range and its description in each line and press Enter. Use a semicolon (;) to separate the address and its description;
	  • Click next to the table header **Type** or **Member** to filter excluded address members by type or content.
	Note: Excluded members' address range needs to be in the address range of the members, otherwise the configuration cannot be completed.

Basic	
Delete	Delete the selected excluded member from the list.

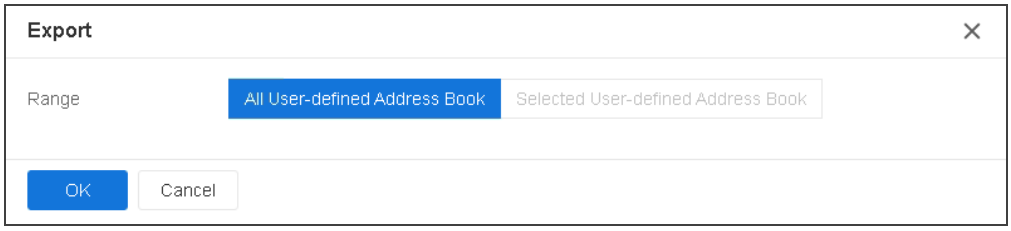
3. Click OK.

Exporting User-defined Address Books

You can export user-defined address books from the device to your PC as a .dat file. This way, the .dat file can be imported to another device.

To export user-defined address books, take the following steps:

1. Select **Object** > **Address Book**.
2. You can select all user-defined address books or selected address books.



   - Export all user-defined address books: Click **Export**. In the Range field, select **All User-defined Address Book** to export all user-defined address books from the device.
   - Export selected user-defined address books: In the address book list, select one or more address books that you want to export, click **Export**, and then select **Selected User-defined Address Book** in the Range field to export these selected address books.

3. Click **OK**.

Notes: Only user-defined address books can be exported.

Importing User-defined Address Books

You can import address book entries from your PC to the device. This reduces the workload of manually creating address book entries. Only .dat files can be imported.

To import the configuration file of user-defined address books, take the following steps:

1. Select **Object** > **Address Book**.
2. Click **Import**.



3. Click **Browse** and select the configuration file of address books that is saved on your PC.
4. Click **OK**. The imported address books are displayed on the **Address Book** page.

Notes: You need to import a configuration file whose address book entry parameters are consistent with that in the device. We recommend that you use a file exported from the device as the template and modify this template based on your requirements.

Viewing Details

To view the details of an address entry, take the following steps, including the name, member, description and reference:

1. Click **Object>Address Book**.
2. In the Address Book dialog box, select "+" before an address entry from the member list, and view the details under the entry.

Searching Address Entries

Use the Filter to search for the address entries that match the filter conditions. The filter conditions include the address entry name, IP address of the members, the description, ordered member address and whether the entry is referenced by other function modules. Among them, whether it is a filtering condition for ordered member address needs to enable the ordered address book function before it can be used. How to enable the ordered address book function, please refer to the address book global configuration.

1. Click **Object > Address Entry**.
2. At the top-right corner of the page, click **Filter**. Then a new row appears at the top.
3. Click **+Filter** to add a new filter condition. Then select a filter condition from the drop-down menu and enter a value.
4. Press **Enter** to search for the service entry that matches the filter conditions.
5. Repeat the above two steps to add more filter conditions. The relationship between each filter condition is **AND**.
6. To delete a filter condition, hover your mouse on that condition and then click the × icon.

   To close the filter, click the × icon on the right side of the row.

Save the filter conditions.

1. After adding the filter conditions, click the **+ Filter** after the next arrow, in the drop-down menu, click **Save Filters**.
2. Specifies the name of the filter condition to save, the maximum length of name is 32 characters, and the name supports only Chinese and English characters and underscores.
3. Click the **Save** button on the right side of the text box.

4. To use the saved filter condition, double click the name of the saved filter condition.

5. To delete the saved filter condition, click × on the right side of the filter condition.



Notes:

- You can add up to 20 filter conditions as needed.
- After the device has been upgraded, the saved filter condition will be cleared.

Device Object

You can categorize one or more IoT devices into a device collection based on multiple dimensions of the device (including the manufacturer, type, model, and operating system of the device) and assign a device object name to the device collection. The system maps the identified IoT device information with the device object attributes, and then the security policy can directly reference the device object name to control the IoT device collection.



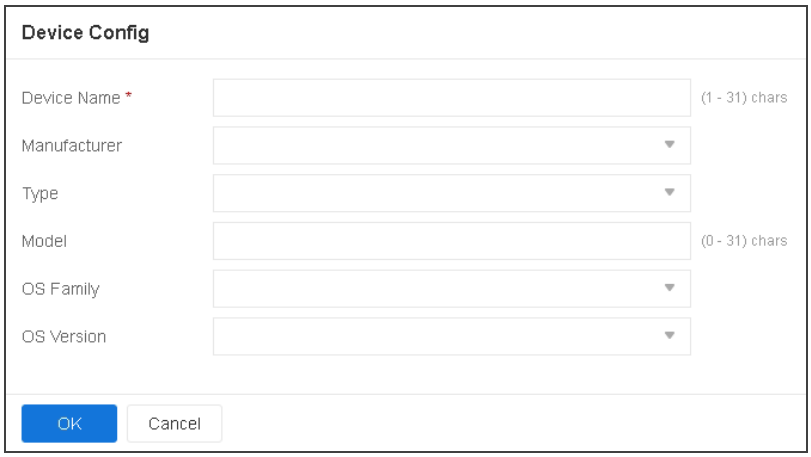
Notes: The device object can be configured only after you install an IoT control license.

Configuring a Device Object

Creating a Device Object

To create a device object, take the following steps:

1. Select **Object** > **Device**.
2. Click **New**.



Option	Description
Device Name	Enter the name of the device object, which needs to be 1 to 31 characters in length.
Manufacturer	Select the manufacturer type and manufacturer name. • Predefined: Select **Predefined** and then select a manufacturer name in the list below. You can also search for a predefined manufacturer name in the search box. • User-defined: Select **User-defined**, enter a custom manufacturer name, and then click **Add**.
Type	Select the device type and type name.

Option	Description
	• Predefined: Select **Predefined** and then select a device type name in the list below. You can also search for a predefined device type name in the search box. • User-defined: Select **User-defined**, enter a custom device type name, and then click **Add**.
Model	Specifies the model of the device, which cannot exceed 31 characters in length.
OS Family	Select the OS family type and name. • Predefined: Select **Predefined** and then select an OS family name in the list below. You can also search for a predefined OS family name in the search box. • User-defined: Select **User-defined**, enter a custom OS family name, and then click **Add**.
OS Version	Select the corresponding OS version. • Predefined: Select **Predefined** and then select an OS version in the list below. You can also search for a predefined OS version in the search box. • User-defined: Select **User-defined**, enter a custom OS family version, and then click **Add**.

3. Click **OK**. The newly create device object is displayed in the list.

Editing a Device Object

To edit a device object, take the following steps:

1. Select **Object** > **Device**.
2. In the device list, select the device object that you want to edit and click **Edit**.
3. On the **Device Config** page, edit the configuration.

Deleting a Device Object

To delete a device object, take the following steps:

1. Select **Object** > **Device**.
2. In the device list, select the device object that you want to delete and click **Delete**.

Viewing the Mapping IP Details of Device

To view the mapping IP details of device, take the following steps:

1. Select **Object** > **Device**.
2. Click "+" to the left of a device object name whose details you want to view.
3. In the **Device Mapping IP** section, view the details.

Host Book

You can specify a name to be a collection of one domain name or several domain names, and reference this host book when configuring. Host book is the database to store the relationships of domain integrations and the specified names in system.

The entry of the relationship of domain integrations and the specified name is called host entry.

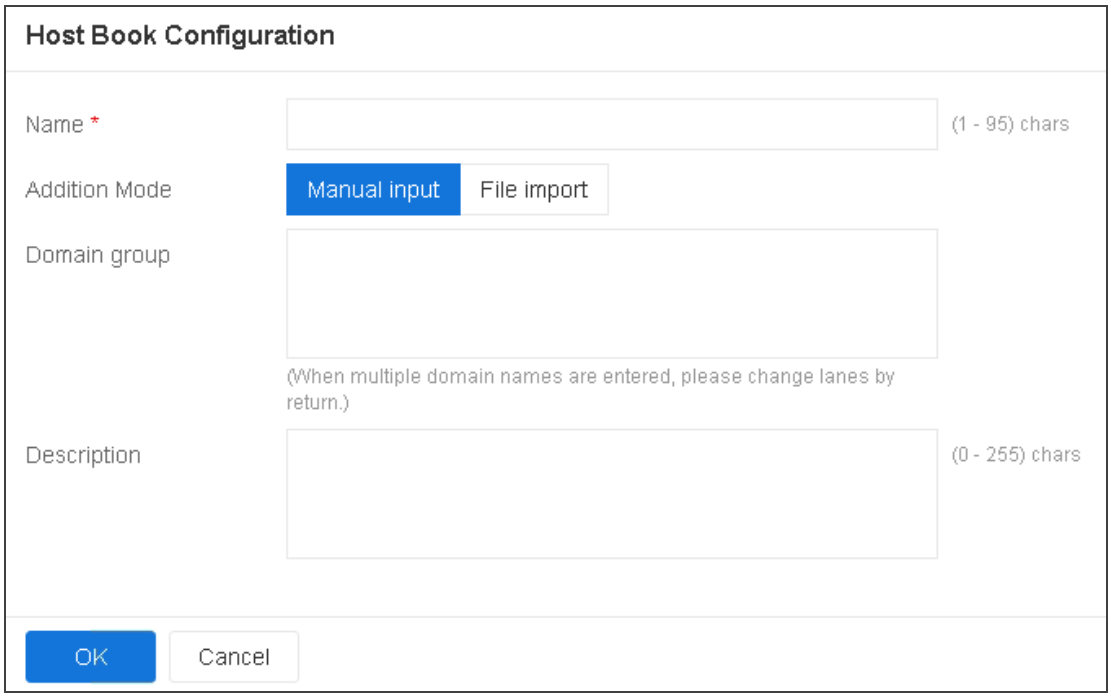


Notes: The maximum number of host entries is one fourth of the maximum number of address entries.

Creating a Host Book

To create a host book, take the following steps:

1. Select **Object > Host Book**.
2. Click **New**.



Option	Description
Name	Type a name for the host book.
Description	Type the description of host book entry.
Addition Mode	Specify the mode for adding domain members. • Manual input: Add the domain member to the host book via inputting IP address or domain manually. • File import: Add a batch of domain members to the host book via importing the file.

Option	Description
Domain Group	When the "Manual input" is selected, enter the IP address or domain names of the domain member. **Note**: Press **Enter** to separate several domain members.
File Name	When the "File import" is selected, click **Browser** to upload a domain name file in the local. **Note**: Only the UTF-8 encoding file (*.txt or *.csv) can be imported currently.

3. Click **OK**.

Editing a Host Book

To edit a host book, take the following steps:

1. Select **Object** > **Host Book**, and enter the **Host Book** page.
2. In the host book list, select a host book entry to edit and click **Edit**.
3. In the **Host Book Configuration** dialog, edit the selected host book entry as needed.

Notes: When you edit a host book entry, if you add more domain members via importing a file, the domain in the file will cover all the domain members in the selected entry.

Deleting a Host Book

To delete a host book, take the following steps:

1. Select **Object** > **Host Book**, and enter the **Host Book** page.
2. In the host book list, select a host book entry to delete and click **Delete**.

Viewing Details

To view details about a host book entry, take the following steps:

1. Select **Object** > **Host Book**.
2. In the host book list, select "+" before a host book entry, and view the details under the entry.

Details	
Name	Displays the name of the host book.
Member	Displays the domain name members in the host book.
Description	Displays the description about the host book.
Referenced by	
DNS Proxy	Displays the information referenced by the DNS proxy rule.
Policy	Displays the ID of the policy that references the host book. You can click the ID to view the policy details.
Outbound Rule	Displays the information referenced by the outbound rule.
DNS Rewrite	Displays the information referenced by the DNS rewrite rule.

Custom IP Geolocation

IP geolocation indicates geographical location of IP address, such as the country or region where the IP address resides. The IP geolocation database of the system provides the mapping between IP addresses and their geolocations. In addition, the system supports the custom IP geolocation function. You can customize the geographical location of IP addresses. For example, when the geographical location of the IP address is invalid, you can customize this information.

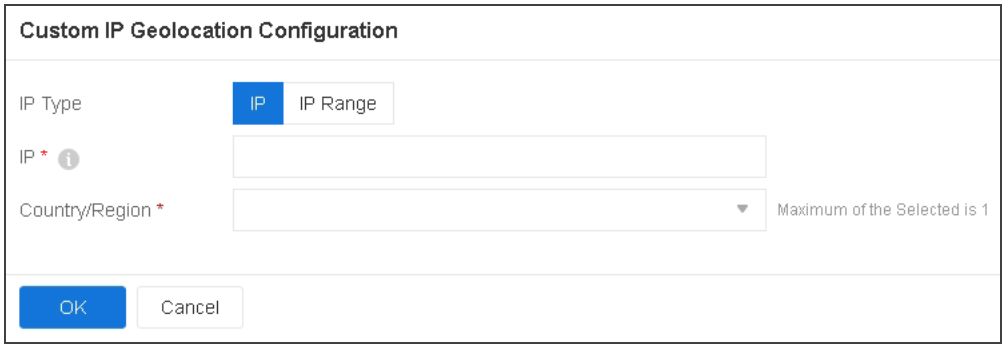
Notes:

- You can configure custom IP geolocation for only public IPv4 address.
- When you query the geographical location of IP addresses, the system preferentially queries the custom geographical location.

Creating a Custom IP Geolocation

To create a custom IP geolocation, take the following steps:

1. Select **Object** > **Custom IP Geolocation**.
2. Click **New**.



Option	Description
IP Type	Specifies the IP type of the custom geolocation. Valid values:

Option	Description
	IP and IP Range. When you select IP, you need to enter an IP address in the IP field. When you select IP Range, you need to enter a start IP address and an end IP address in the IP Range fields.
Country/Region	Specifies the geolocation of the IP address. To do this, select a country/region name from the drop-down list. The selected country/region will be displayed in the field. If you select CN China, you can click "+" to the left of CN China to select the province and city. **Note**: You cannot select a province or city for devices of the oversea version.

3. Click **OK**. The newly created custom IP geolocation will be displayed in the custom IP geolocation list.



Notes: You can configure up to 256 custom IP geolocation entries in the system.

Editing a Custom IP Geolocation

To edit a custom IP geolocation, take the following steps:

1. Select **Object** > **Custom IP Geolocation**.
2. In the custom IP geolocation list, select the custom IP geolocation that you want to edit and click **Edit**.
3. On the **Custom IP Geolocation Configuration** page, edit the configuration of the custom IP geolocation.

Deleting a Custom IP Geolocation

To delete a custom IP geolocation, take the following steps:

1. Select **Object** > **Custom IP Geolocation**.
2. In the custom IP geolocation list, select the custom IP geolocation that you want to delete and click **Delete**.

Querying Geolocation

To query the geolocation of an IP address, take the following steps:

1. Select **Object** > **Custom IP Geolocation**.
2. Click **Location Lookup**.
3. In the **Location Lookup** panel, enter the IP address to be queried and click **Inquiry**. The geolocation of the IP address will be displayed in the text box below.

Filtering Custom IP Geolocation Entries

You can use the filter to search for custom IP geolocation entries that meets the filter conditions. The filter conditions include Location, IP Address, and Redundant or not. If the Redundant or not condition is set to yes, it indicates that the custom geolocation of the IP address is consistent with the geolocation of the IP address in the IP geolocation database.

To filter custom IP geolocation entries, take the following steps:

1. Select **Object** > **Custom IP Geolocation**.
2. Click **Filter**, select a filter condition from the drop-down list, and then enter or select a corresponding value.
3. After you enter or select a value, the custom IP geolocation entries that meet the filter conditions will be displayed in the list below.

4. Repeat the steps above to add more filter conditions. The logical relation between filter conditions is AND.

5. To delete a filter condition, hover your mouse over the filter condition and click "×"。 To delete all filter conditions, click "×Remove All" at the end of this row.

Service Book

Service is an information stream designed with protocol standards. Service has some specific distinguishing features, like corresponding protocol, port number, etc. For example, the FTP service uses TCP protocol, and its port number is 21. Service is an essential element for the configuration of multiple StoneOS modules including policy rules, NAT rules, QoS rules, etc.

System ships with multiple predefined services/service groups. Besides, you can also customize user-defined services/service groups as needed. All these service/service groups are stored in and managed by StoneOS service book.

Predefined Service/Service Group

System ships with multiple predefined services, and identifies the corresponding application types based on the service ports. The supported predefined services may vary from different Hillstone device models. Predefined service groups contain related predefined services to facilitate user configuration.

User-defined Service

Except for the above predefined services, you can also create your own user-defined services easily. The parameters that will be specified for the user-defined service entries include:

- Name
- Protocol type
- The source and destination port for TCP or UDP service, and the type and code value for ICMP service.

User-defined Service Group

You can organize some services together to form a service group, and apply the service group to StoneOS policies directly to facilitate management. The service group has the following features:

- Each service of the service book can be used by one or more service groups.
- A service group can contain both predefined services and user-defined services.
- A service group can contain another service group. The service group of StoneOS supports up to 8 layers of nests.

The service group also has the following limitations:

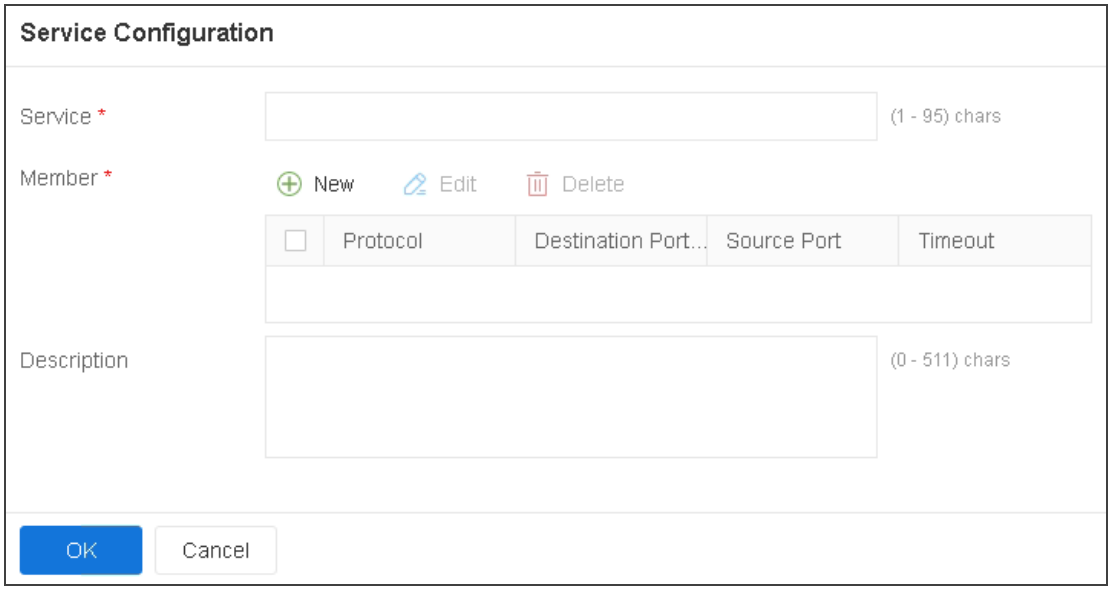
- The name of a service and service group should not be identical.
- A service group being used by any policy cannot be deleted. To delete such a service group, you must first end its relationship with the other modules.
- If a user-defined service is deleted from a service group, the service will also be deleted from all of the service groups using it.

Configuring a Service Book

This section describes how to configure a user-defined service and service group.

Configuring a User-defined Service

1. Select **Object > Service Book > Service**.
2. Click **New**.



Service Configuration	
Service	Type the name for the user-defined service into the textbox.
Member	Specify a protocol type for the user-defined service. The available options include TCP, UDP, ICMP, ICMPv6 and All. If needed, you can add multiple service items. Click **New** and the parameters for the protocol types are described as follows:
	TCP/UDP Destination port: • Min - Specifies the minimum port number of the specified service entry. • Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535. Source port: • Min - Specifies the minimum port number of

Service Configuration		
		the specified service entry. • Max - Specifies the maximum port number of the specified service entry. The value range is 0 to 65535.  Notes: • The minimum port number cannot exceed the maximum port number. • The "Min" of the destination port is required, and other options are optional. • If "Max " is not configured, system will use "Min" as the single code.
	ICMP	Type: Specifies an ICMP type for the service entry. The value range is 0（Echp-Reply）, 3（Destination-Unreachable）, 4（Source Quench）, 5（Redirect）, 8（Echo）, 11（Time Exceeded）, 12（Parameter Problem）, 13（Timestamp）, 14（Timestamp Reply）, 15（Information Request）, 16（Information Reply）, 17（Address Mask Request）, 18

Service Configuration		
		（Address Mask Reply），30（Traceroute），31（Datagram Conversion Error），32（Mobile Host Redirect），33（IPv6 Where-Are-You），34（IPv6 I-Am-Here），35（Mobile Registration Request），36（Mobile Registration Reply）. Code: Specifies a minimum value and maximum value for ICMP code. The value range is 0 to 15, the default value is : min code - 0, max code - 15.  Notes: • The minimum code cannot exceed the maximum code. • If "Max " is not configured, system will use "Min" as the single code.
	ICMPv6	Type: Specifies an ICMPv6 type for the service entry. The value range is 1（Dest-Unreachable），2（Packet Too Big），3（Time Exceeded），4（Parameter Problem），5-99 (Unallocated Error message), 100（Private experimentation），101（Private experimentation），102-126 (Unallocated Error message), 127（Reserved for expansion of ICMPv6 error message），128（Echo

Service Configuration	
	Request）, 129（Echo Reply）, 130（Multicast Listener Query）, 131（Multicast Listener Report）, 132（Multicast Listener Done）, 133（Router Solicitation）, 134（Router Advertisement）, 135（Neighbor Solicitation）, 136（Neighbor Advertisement）, 137（Redirect Message）, 138（Router Renumbering）, 139（ICMP Node Information Query）, 140（ICMP Node Information Response）, 141（Inverse Neighbor Discovery Solicitation Message）, 142（Inverse Neighbor Discovery Advertisement Message）, 143（Version 2 Multicast Listener Report）, 144（Home Agent Address Discovery Request Massage）, 145（Home Agent Address Discovery Reply Massage）, 146（Mobile Prefix Solicitation）, 147（Mobile Prefix Advertisement ）, 148（Certification Path Solicitation Message）, 149（Certification Path Advertisement Message）, 150（ICMP message utilized by experimental mobility protocols such as Seamoby）, 151（Multicast Router Advertisement）, 152（Multicast Router Solicitation ）, 153（Multicast Router Termination）, 154（FMIPv6 Messages）, 200（Private experimentation）, 201（Private experimentation）and 255（Reserved for expansion of

Service Configuration	
	All Protocol: Specifies a protocol number for the service entry. The value range is 1 to 255.
Description	If it's needed, type the description for the service into the text box.

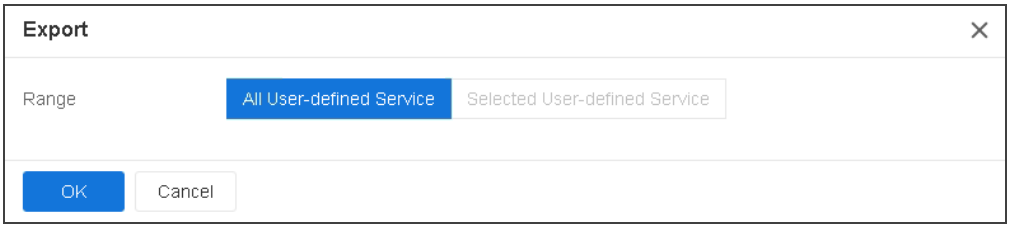
3. Click **OK**.

Exporting User-defined Services

You can export user-defined services from the device to your PC as a .dat file. This way, the .dat file can be imported to another device.

To export user-defined services, take the following steps:

1. Select **Object** > **Service Book** > **Service**.
2. You can select all user-defined services or selected services.



- Export all user-defined services: Click **Export**. In the Range field, select **All User-defined Service** to export all user-defined services from the device.
- Export selected user-defined services: In the service list, select one or more services that you want to export, click **Export**, and then select **Selected User-defined Service** in the Range field to export these selected services.

3. Click **OK**.

Notes: Only user-defined services can be exported.

Importing User-defined Services

You can import service entries from your PC to the device. This reduces the workload of manually creating service entries. Only .dat files can be imported.

To import the configuration file of user-defined services, take the following steps:

1. Select **Object** > **Service Book** > **Service**.
2. Click **Import**.



3. Click **Browse** and select the configuration file of services that is saved on your PC.
4. Click **OK**. The imported services are displayed on the **Service** page.

Notes: You need to import a configuration file whose service entry parameters are consistent with that in the device. We recommend that you use a file exported from the device as the template and modify this template based on your requirements.

Configuring a User-defined Service Group

1. Select **Object > Service Book > Service Group**.
2. Click **New**.



Service Group Configuration	
Name	Type the name for the user-defined service group into the text box.
Description	If needed, type the description for the service into the text box.
Member Type	Add services or service groups to the service group. System supports at most 8-layer nested service group. Expand Pre-defined Service or User-defined Service from the left pane, select services or service groups, and then click **Add** to add them to the right pane. To remove a selected service, select it from the right pane, and then click **Remove**.

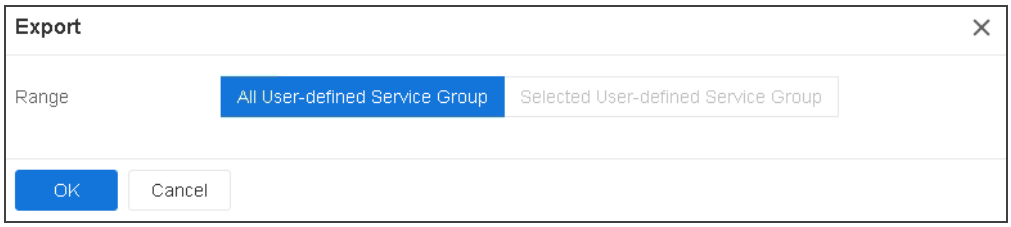
3. Click **OK**.

Exporting User-defined Service Groups

You can export user-defined service groups from the device to your PC as a .dat file. This way, the .dat file can be imported to another device.

To export user-defined service groups, take the following steps:

1. Select **Object** > **Service Book** > **Service Group**.
2. You can select all user-defined service groups or selected service groups.



   - Export all user-defined service groups: Click **Export**. In the Range field, select **All User-defined Service Group** to export all user-defined service groups from the device.
   - Export selected user-defined service groups: In the service group list, select one or more service groups that you want to export, click **Export**, and then select **Selected User-defined Service Group** in the Range field to export these selected service groups.

3. Click **OK**.

Notes: Only user-defined service groups can be exported.

Importing User-defined Service Groups

You can import service group entries from your PC to the device. This reduces the workload of manually creating service group entries. Only .dat files can be imported.

To import the configuration file of user-defined service groups, take the following steps:

1. Select **Object** > **Service Book** > **Service Group**.
2. Click **Import**.



3. Click **Browse** and select the configuration file of service groups that is saved on your PC.
4. Click **OK**. The imported service groups are displayed on the **Service Group** page.

Notes: You need to import a configuration file whose service group entry parameters are consistent with that in the device. We recommend that you use a file exported from the device as the template and modify this template based on your requirements.

Viewing Details

To view the details of a service entry, take the following steps, including the name, protocol, destination port and reference:

1. Click **Object>Service Book** > **Service**.
2. In the service dialog box, select an address entry from the member list, and view the details under the list.

Searching Service Entries

Use the Filter to search for the service entries that match the filter conditions. The filter conditions include service type, name, protocol, destination port and source port, and whether the service entry is referenced by other function modules.

1. Click **Object > Service Book > Service**.
2. At the top-left corner of the **Service** page, click **Filter**.
3. Click **+ Filter** to add a new filter condition. Then select a filter condition from the drop-down menu and enter a value.
4. Press **Enter** to search for the service entry that matches the filter conditions.
5. Repeat the above two steps to add more filter conditions. The relationship between each filter condition is **AND**.
6. To delete a filter condition, hover your mouse on that condition and then click the × icon. To close the filter, click the × icon on the right side of the row.



Save the filter conditions.

1. After adding the filter conditions, click the **+ Filter** after the next arrow, in the drop-down menu, click **Save Filters**.
2. Specifies the name of the filter condition to save, the maximum length of name is 32 characters, and the name supports only Chinese and English characters and underscores.
3. Click the **Save** button on the right side of the text box.
4. To use the saved filter condition, double click the name of the saved filter condition.
5. To delete the saved filter condition, click × on the right side of the filter condition.

Notes:

- You can add up to 20 filter conditions as needed.
- After the device has been upgraded, the saved filter condition will be cleared.

Searching Service Groups

Use the Filter to search for the service groups that match the filter conditions. The filter conditions include service group name, type, and whether the service group is referenced by other function modules.

1. Click **Object > Service Book > Service Group**.
2. At the top-left corner of the page, click **Filter**. Then a new row appears at the top.
3. Click **Filter** to add a new filter condition. Then select a filter condition from the drop-down menu and enter a value.
4. Press **Enter** to search for the service group that matches the filter conditions.
5. Repeat the above two steps to add more filter conditions. The relationship between each filter condition is **AND**.
6. To delete a filter condition, hover your mouse on that condition and then click the × icon.

   To close the filter, click the × icon on the right side of the row.

Save the filter conditions.

1. After adding the filter conditions, click the **Filter** after the next arrow, in the drop-down menu, click **Save Filters**.
2. Specifies the name of the filter condition to save, the maximum length of name is 32 characters, and the name supports only Chinese and English characters and underscores.
3. Click the **Save** button on the right side of the text box.

4. To use the saved filter condition, double click the name of the saved filter condition.

5. To delete the saved filter condition, click × on the right side of the filter condition.



Notes:

- You can add up to 20 filter conditions as needed.
- After the device has been upgraded, the saved filter condition will be cleared.

Application Book

Application has some specific features, like corresponding protocol, port number, application type, etc. Application is an essential element for the configuration of multiple device modules including policy rules, NAT rules, application QoS management, etc.

System ships with multiple predefined applications and predefined application groups. Besides, you can also customize user-defined application and application groups as needed. All of these applications and applications groups are stored in and managed by StoneOS application book. On the **Object** > **Application Book** > **Application** page, deprecated predefined applications are marked with a strikethrough, which cannot be edited or deleted. If a deprecated predefined application is referenced by other functional module, an error is returned.

Editing a Predefined Application

You can view and use all the supported predefined applications and edit configurations such as TCP timeout, but cannot delete any of them. To edit a predefined application, take the following steps:

1. Select **Object > Application Book > Application**.
2. Select the application you want to edit from the application list, and click **Edit**.
3. In the Application Configuration dialog box, edit configurations such as TCP timeout and signatures for the application.

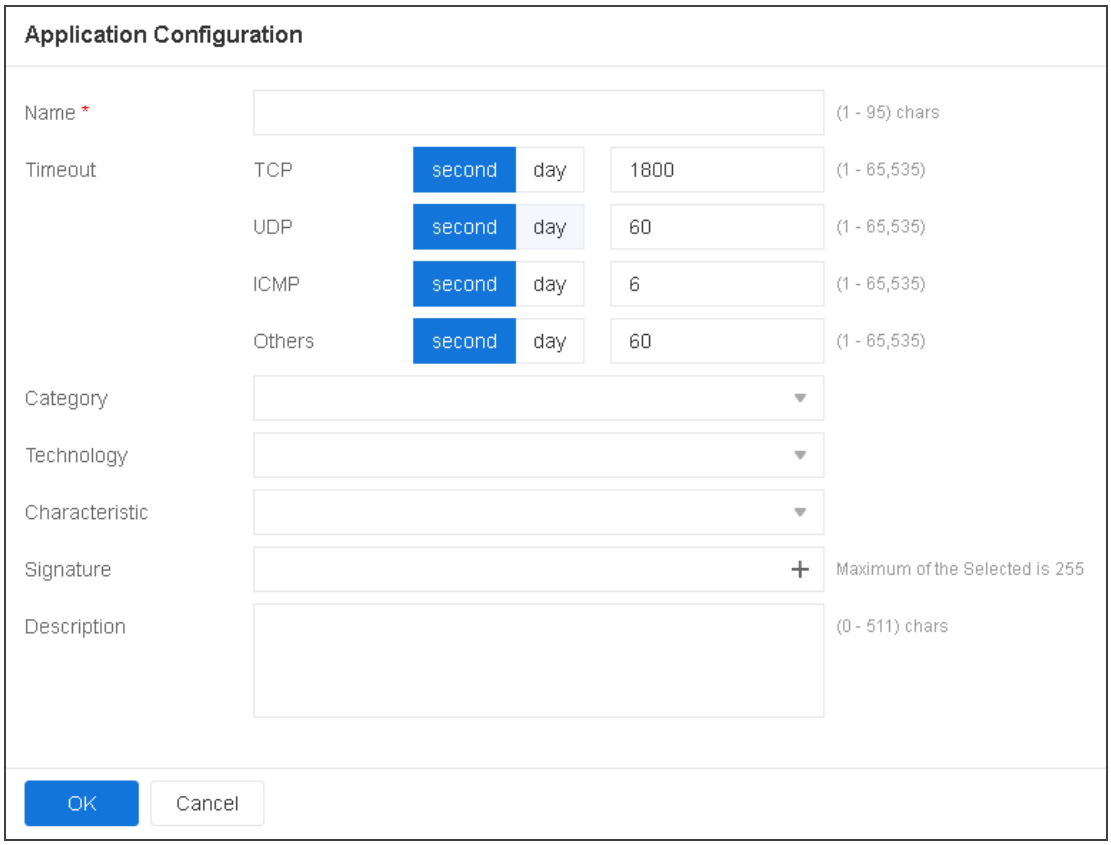
Creating a User-defined Application

You can create your own user-defined applications. By configuring the customized application signature rules, system can identify and manage the traffic that crosses into the device, thus identifying the type of the traffic.

To create a user-defined application, take the following steps:

1. Select **Object > Application Book > Application**.

2. Click **New**.



Option	Description
Name	Specifies the name of the user-defined application.
Timeout	Configures the application timeout value. If not, system will use the default value of the protocol.

Option	Description
Category	Specifies the category of the user-defined application. The categories and subcategories are maintained by the application signature database. The category corresponds to the application group of level 1 in the signature database and the subcategory corresponds to the application group of level 2 under level 1. You can configure a category for each user-defined application. By default, user-defined applications are not configured with a category.
Subcategory	Specifies the subcategory of the user-defined application. You can configure only one subcategory for the application. By default, user-defined applications are not configured with a subcategory.
Technology	Specifies the technology used by the user-defined application. The technologies used by applications are maintained by the application signature database. You can configure only one technology for the application. By default, user-defined applications are not configured with a technology.
Characteristic	Specifies the characteristic of the user-defined application. The characteristics are maintained by the application signature database. You can configure one or more characteristics. By default, user-defined applications are not configured with a characteristic.
Signature	Select the signature of the application and then click **Add**. To create a new signature, see "Creating a Signature Rule" on Page

Option	Description
	859.
Description	Specify the description of the user-defined application.

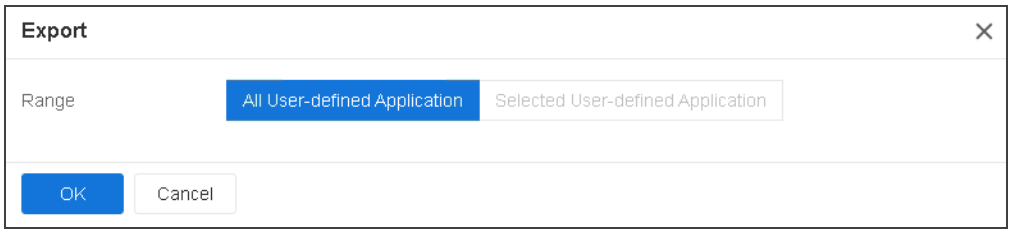
3. Click **OK**.

Exporting User-defined Applications

You can export user-defined applications from the device to your PC as a .dat file. This way, the .dat file can be imported to another device.

To export user-defined applications, take the following steps:

1. Select **Object** > **Application Book** > **Application**.
2. You can select all user-defined applications or selected applications.



- Export all user-defined applications: Click **Export**. In the Range field, select **All User-defined Application** to export all user-defined applications from the device.
- Export selected user-defined applications: In the application list, select one or more applications that you want to export, click **Export**, and then select **Selected User-defined Application** in the Range field to export these selected applications.

3. Click **OK**.

Notes: Only user-defined applications can be exported.

Importing User-defined Applications

You can import application entries from your PC to the device. This reduces the workload of manually creating application entries. Only .dat files can be imported.

To import the configuration file of user-defined applications, take the following steps:

1. Select **Object** > **Application Book** > **Application**.
2. Click **Import**.



3. Click **Browse** and select the configuration file of applications that is saved on your PC.
4. Click **OK**. The imported applications are displayed on the **Application** page.

Notes: You need to import a configuration file whose application entry parameters are consistent with that in the device. We recommend that you use a file exported from the device as the template and modify this template based on your requirements.

Creating a User-defined Application Group

To create a user-defined application group, take the following steps:

1. Select **Object > Application Book > Application Groups**.
2. Click **New**.



Option	Description
Name	Specifies a name for the new application group.
Member	Select an application, application group, or application filter that you want to add to the application group. To search for an application, you can enter the name of the application. To delete an added application, click **X**. **Note**: Deprecated predefined applications cannot be added.
Description	Specifies the description for the application group.

3. Click **OK**.

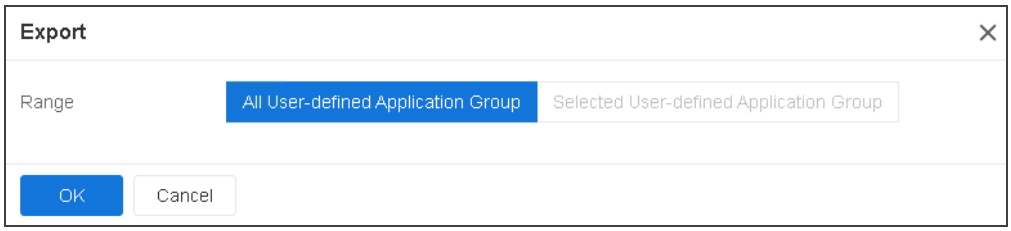
Exporting User-defined Application Groups

You can export user-defined application groups from the device to your PC as a .dat file. This way, the .dat file can be imported to another device.

To export user-defined application groups, take the following steps:

1. Select **Object** > **Application Book** > **Application Groups**.

2. You can select all user-defined application groups or selected application groups.



   - Export all user-defined application groups: Click **Export**. In the Range field, select **All User-defined Application Group** to export all user-defined application groups from the device.

   - Export selected user-defined application groups: In the application group list, select one or more application groups that you want to export, click **Export**, and then select **Selected User-defined Application Group** in the Range field to export these selected application groups.

3. Click **OK**.

Notes: Only user-defined application groups can be exported.

Importing User-defined Application Groups

You can import application group entries from your PC to the device. This reduces the workload of manually creating application group entries. Only .dat files can be imported.

To import the configuration file of user-defined application groups, take the following steps:

1. Select **Object** > **Application Book** > **Application Groups**.

2. Click **Import**.



3. Click **Browse** and select the configuration file of application groups that is saved on your PC.

4. Click **OK**. The imported application groups are displayed on the **Application Groups** page.

Notes: You need to import a configuration file whose application group entry parameters are consistent with that in the device. We recommend that you use a file exported from the device as the template and modify this template based on your requirements.

Creating an Application Filter Group

Application Filter Group allows you to create a group to filter applications according to application category, sub-category, technology, risk, and attributes.

To create an application filter group, take the following steps:

1. Select **Object** > **Application Book** > **Application Filters**.

2. Click **New**.

3. Type an application filter group name in the Name text box.

4. Specifies the filter condition. Choose the category, subcategory, technology, risk or characteristic from the drop-down list and then select a condition under the corresponding filter. You can add multiple filters based on your needs.

5. Click **OK**.

Creating a Signature Rule

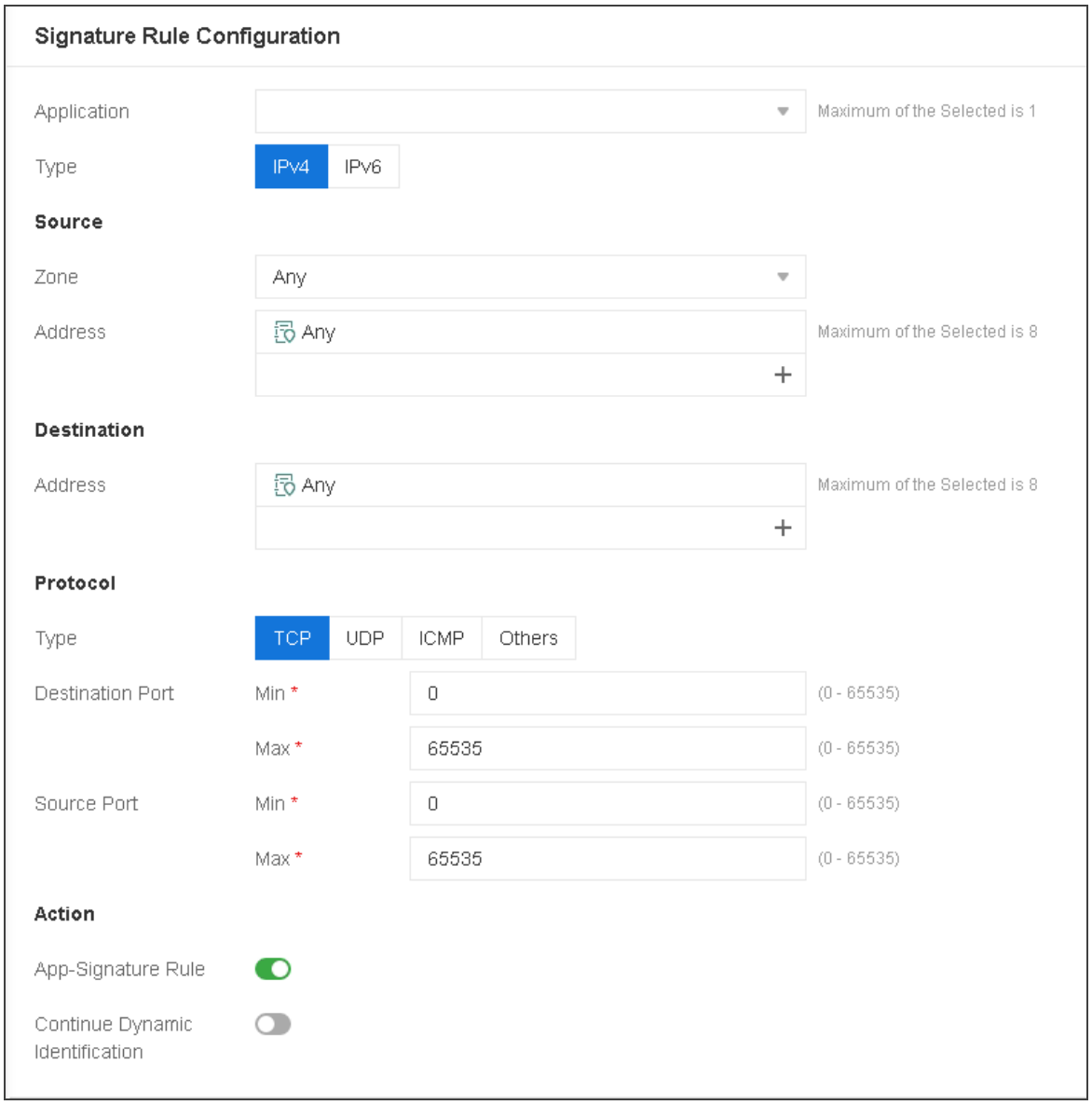
By configuring the customized application signature rules, system can identify and manage the traffic that crosses into the device. When the traffic matches all of the conditions defined in the signature rule, it hits this signature rule. Then system identifies the application type.

If IPv6 is enabled, traffic of IPv6 address will be recognized by StoneOS.

To create a new signature rule, take the following steps:

1. Select **Object > Application Book > Static Signature Rule**.

2. Click **New**.



Option	Description
Application	Select the name of the application (including both predefined and custom applications) to which the configured signature rule applies. Once configured, traffic that meets all the conditions of

Option	Description
	the signature rule is identified as this application. **Note**: Deprecated predefined applications cannot be added.
Type	Specify the IP address type, including IPv4 and IPv6 address. If IPv6 is enabled, traffic of IPv6 address will be recognized by StoneOS.
Source	
Zone	Specify the source security zone of the signature rule.
Address	Specify the source address. You can use the Address Book type or the IP/Netmask type. You can also perform the following operation: • You can click in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member

Option	Description
	1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched.
Destination	
Address	Specify the source address. You can use the Address Book type or the IP/Netmask type. You can also perform the following operation: • You can click in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched.
Protocol	

Option	Description
Enable	Select the **Enable** button to configure the protocol of the signature rule.
Type	When selecting **TCP** or **UDP**, • Destination Port: Specify the destination port number of the user-defined application signature. If the destination port number is within a range, system will identify the value of min-port as the minimum port number and identify the value of max-port as the maximum port number. The range of destination port number is 0 to 66535. The port number cannot be 0. For example, the destination port number is in the range of 0 to 20, but it cannot be 0. • Source Port: Specify the source port number of the user-defined application signature. If the source port number is within a range, system will identify the value of min-port as the minimum port number and identify the value of max-port as the maximum port number. The range of source port number is 0 to 66535. When selecting **ICMP** or **ICMPv6**: • When IPv4 is selected, select **ICMP**: • Type: Specify the value of the ICMP type of the application signature. The options are as follows: is 0（Echp-Reply）, 3（Destination-Unreachable）,

Option	Description
	4（Source Quench）, 5（Redirect）, 8（Echo）, 11（Time Exceeded）, 12（Parameter Problem）, 13（Timestamp）, 14（Timestamp Reply）, 15（Information Request）, 16（Information Reply）, 17（Address Mask Request）, 18（Address Mask Reply）, 30（Traceroute）, 31（Datagram Conversion Error）, 32（Mobile Host Redirect）, 33（IPv6 Where-Are-You）, 34（IPv6 I-Am-Here）, 35（Mobile Registration Request）, 36（Mobile Registration Reply）. • Min Code: Specify the value of the minimum ICMP code of the application signature. The minimum ICMP code is in the range of 0 to 15. The default value is 0. • Max Code: Specify the value of the maximum ICMP code of the application signature. The maximum ICMP code is in the range of 0 to 15. The default value is 0. • When IPv6 is selected, select **ICMPv6**: • Type: Specify the value of the ICMPv6 type of the application signature. The options are as follows: 1（Dest-Unreachable）, 2（Packet Too Big）, 3

Option	Description
	（Time Exceeded），4（Parameter Problem），5-99 (Unallocated Error message), 100（Private experimentation），101（Private experimentation），102-126 (Unallocated Error message), 127（Reserved for expansion of ICMPv6 error message），128（Echo Request），129（Echo Reply），130（Multicast Listener Query），131（Multicast Listener Report），132（Multicast Listener Done），133（Router Solicitation），134（Router Advertisement），135（Neighbor Solicitation），136（Neighbor Advertisement），137（Redirect Message），138（Router Renumbering），139（ICMP Node Information Query），140（ICMP Node Information Response），141（Inverse Neighbor Discovery Solicitation Message），142（Inverse Neighbor Discovery Advertisement Message），143（Version 2 Multicast Listener Report），144（Home Agent Address Discovery Request Massage），145（Home Agent Address Discovery Reply Massage），146（Mobile Prefix Solicitation），147（Mobile Prefix Advertisement ），148（Certification Path Solicitation Message），149（Certification Path Advertisement Message），150（ICMP message utilized by exper-

Option	Description
	mination）, 154（FMIPv6 Messages）, 200（Private experimentation）, 201（Private experimentation）and 255（Reserved for expansion of ICMPv6 informational）. • Min Code: Specify the value of the minimum ICMPv6 code of the application signature. The minimum ICMPv6 code is in the range of 0 to 255. The default value is 0. • Max Code: Specify the value of the maximum ICMPv6 code of the application signature. The maximum ICMPv6 code is in the range of 0 to 255. The default value is 0. When selecting **Others**: • Protocol: Specifies the protocol number of the application signature. The protocol number is in the range of 1 to 255.
Action	
App-Signature Rule	Select **Enable** to make this signature rule take effect after the configurations. Otherwise, it will not take effect.
Continue Dynamic Identification	After enabling this function, if the traffic satisfies the user-defined signature rule and system has identified the application type, system will continue identifying the application. To be more accurate, you can enable this function to set the system to

Option	Description
	continue dynamically identification.

3. Click **OK**.

Viewing Details

To view the details of an application entry, including the name, category, subcategory, risk, technology, and reference, take the following steps:

1. Click **Object > Application Book > Application**.
2. In the application dialog box, select "+" before an address entry from the member list, and view the details under the entry.

Application Resource/Application Resource Group

Introduction

Application resource are used to define the applications, content, services, etc. that you want to access. You need to configure parameters such as address, protocol, and port number to specify an application resource entry. Application resource groups are used to define a group of application resources. The system supports to configure a maximum of 256 application resources and 64 application resource groups.

You can define an application resource entry in one of the following ways:

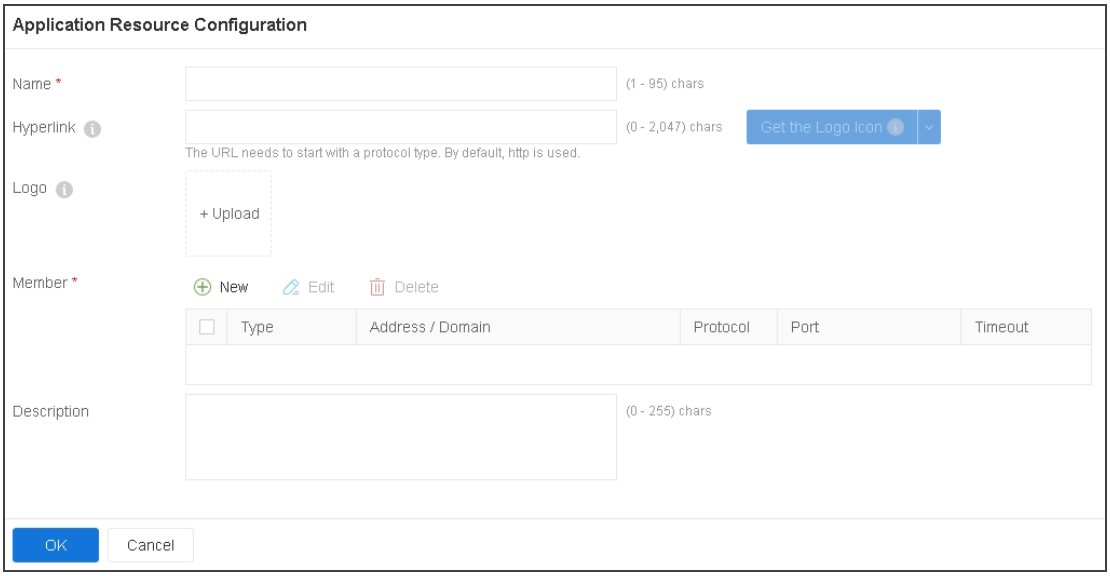
- Based on IP address, protocol, and port number
- Based on IP range, protocol, and port number
- Based on domain name, protocol, and port number

Configuring an Application Resource/Application Resource Group

To configure an application resource, take the following steps:

1. Select **Object** > **Application Resource Book** > **Application Resource**. Or select **ZTNA** > **Application Resource Book** > **Application Resource**.

2. Click **New**.



Option	Description
Name	Type the name of the application resource. The length is 1 to 95 characters.
Hyperlink	Type the hyperlink of the application resource. The length is 0 to 2047 characters. On the ZTNA portal displayed after a user logs in, the user can copy the hyperlink to access an application resource in a browser if the application resource is configured with an hyperlink; or, the user can directly click the application resource icon to access it (make sure the link work). An application resource without a hyperlink configured will not be displayed on the ZTNA portal. If the specified hyperlink does not contain the protocol type, the default HTTP protocol will be used.

Option	Description
	Get the Logo Icon: After a URL is configured, click this button. The system will automatically obtain the logo image corresponding to this URL. If no logo image can be obtained, the "The LOGO Icon is not found" prompt will appear. You can click to select a virtual router to which the URL belongs from the drop-down list.
Logo	Specifies the logo of the application resource, which is used to be displayed on the ZTNA Portal page. To do this, click **Upload** and select an authentication logo from your PC. The logo needs to be in the svg, ico, png, jpg, or jepg format, which cannot exceed 24 KB in size. Note: If you do not upload the logo of the application resource or automatically obtain the logo by configuring a URL, a default logo generated based on the first character of the application resource name is displayed in the application resource list and on the ZTNA Portal page.
Member	Click **New** to add a resource entry and configure the options. Each application resource can contain up to 16 entries. • Type: Specify the address type of the resource entry, including IPv4/Netmask, IPv6/Prefix, IPv4 Range and IPv6 Range and Domain. • Address: Specify the IP address or IP range of the resource entry.

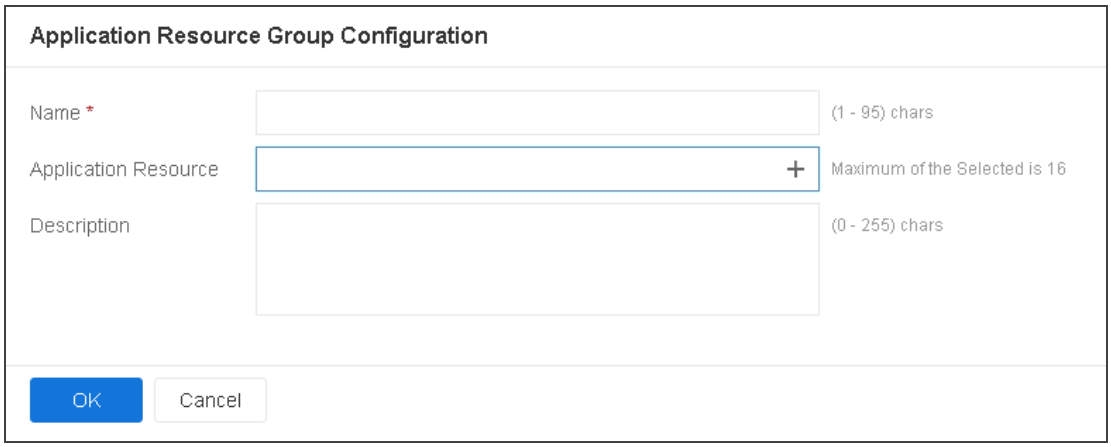
Option	Description
	• Protocol: Specify the protocol type of the resource entry. TCP and UDP are supported for application resources defined based on IP address. HTTP and HTTPS are supported for application resources defined based on domain name. • Port: Specify the port number or port range of the resource entry. If you specify a port number, the minimum port number and the maximum port number need to be the same. The value ranges from 1 to 65535. • Timeout: Specify the timeout value in seconds or days. The value range is 1 to 65535 when it is expressed in seconds and 1 to 1000 when in days. The default value is 1800s when the protocol is TCP, HTTP or HTTPS, and 60s when UDP.
Description	Type description for the application resource. The length is 0 to 255 characters.

3. Click **OK** to save the configuration.
4. On the Application Resource page, by clicking the "+" button in the list to unfold an application resource, you can view more details about it, including the group it belongs to and the ZTNA policy ID that is bound to it.

To configure an application resource group, take the following steps:

1. Select **Object** > **Application Resource Book** > **Application Resource Group**. Or select **ZTNA** > **Application Resource Book** > **Application Resource Group**.

2. Click **New**.



Option	Description
Name	Type the name of the application resource group. The length is 1 to 95 characters.
Application Resource	Select existing application resources. Or, click **New** to create an application resource. You can add up to 16 application resources.
Description	Type description for the application resource group. The length is 0 to 255 characters.

3. Click **OK** to save the configuration.

4. On the Application Resource Group page, by clicking the "+" button to unfold an application resource group, you can view more details about it, including the ZTNA policy ID that is bound to it.

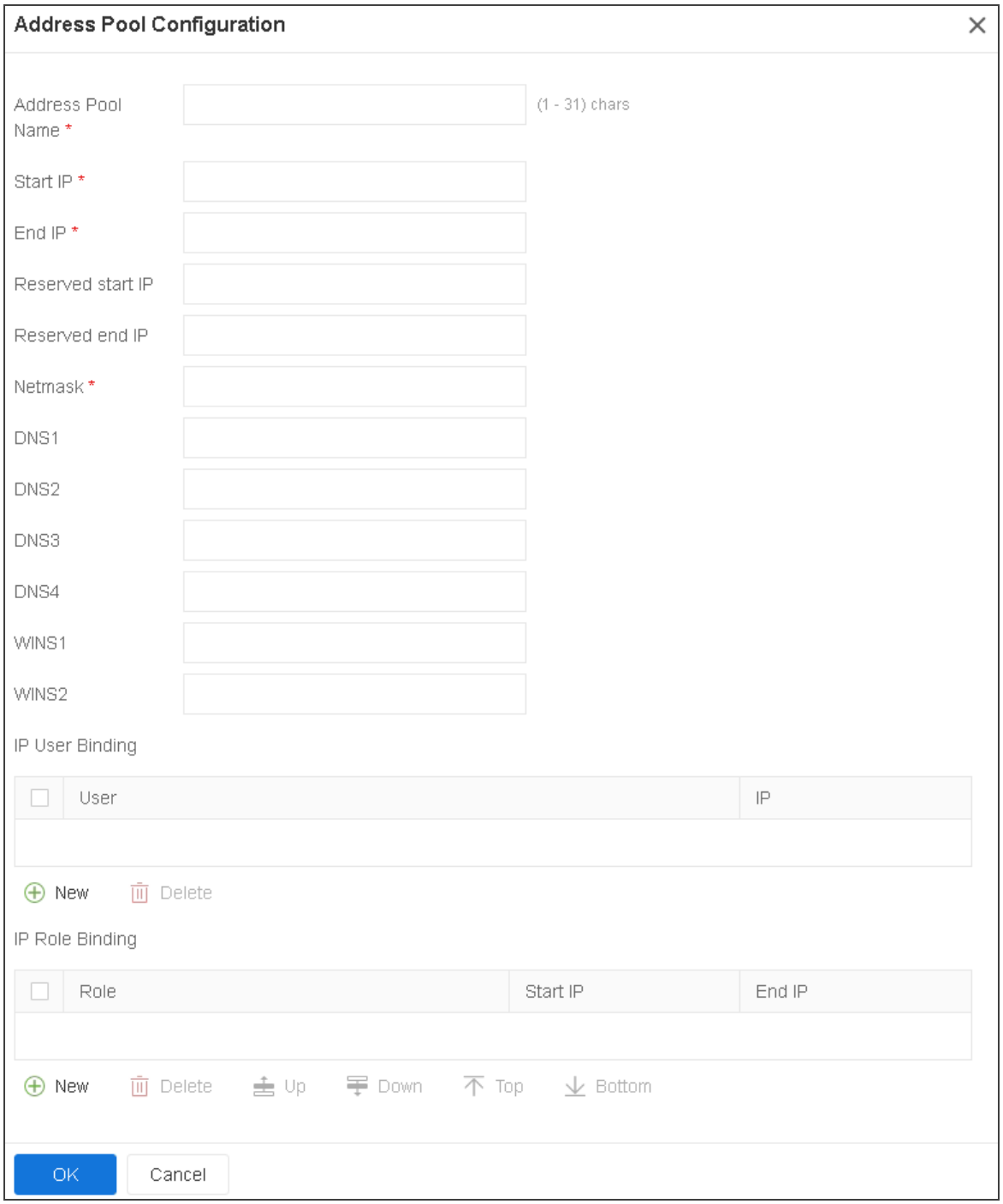
Configuring an Address Pool

To configure an address pool, take the following steps:

1. Select **Object > Access Address Pool**.

2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.

3. Click **New**.



In the Access Address Pool Configuration tab, configure the following options.

Option	Description
Access Address Pool Name	Specifies the name of the address pool.
Start IP	Specifies the start IP of the address pool.
End IP	Specifies the end IP of the address pool.
Reserved start IP	Specifies the reserved start IP of the address pool.
Reserved end IP	Specifies the reserved end IP of the address pool.
Netmask	Specifies the netmask in the dotted decimal format.
Prefix Length	Specifies the prefix for this IPv6 address range. The range is 111 to 128.
DNS1/2/3/4	Specifies the DNS server IP address for the address pool. It is optional. 4 DNS servers can be configured for one address pool at most.
WINS1/2	Specifies the WIN server IP addresses for the address pool. It is optional. Up to 2 WIN servers can be configured for one address pool. This option can only be configured when the created IPv4 address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the **User** box.
IP	Type the IP address into the **IP** box.

Option	Description
New	Click **New** to add an IP user binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Type the role name into the **Role** box.
Start IP	Type the start IP address into the **Start IP** box.
End IP	Type the end IP address into the **End IP** box.
New	Click **New**to add an IP role binding rule.
Delete	To delete a rule, select the rule you want to delete from the list and click **Delete**.
Up/Down/Top/Bottom	System will query IP role binding rules by turn, and allocate the IP address according to the first matched rule. You can move the location up or down at your own choice to adjust the matching sequence accordingly.

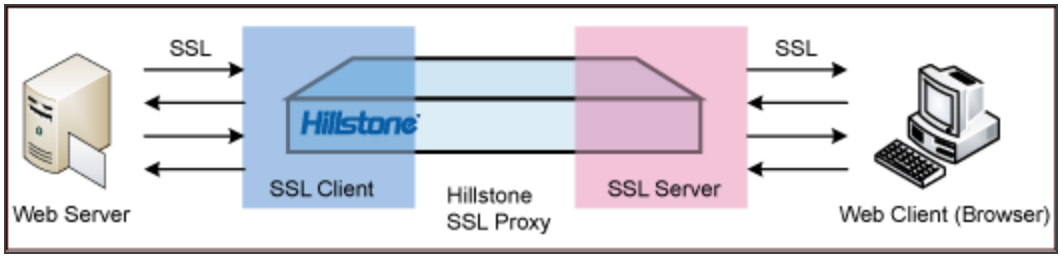
4. Click **OK** to save the settings.

SSL Proxy

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

To assure the security of sensitive data when being transmitting over networks, more and more websites adopt SSL encryption to protect their information. The device provides the SSL proxy function to decrypt HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. The SSL proxy function works in the following two scenarios:

The first scenario, the device works as the gateway of Web clients. The SSL proxy function replaces the certificates of encrypted websites with the SSL proxy certificate to get the encrypted information and send the SSL proxy certificates to the client's Web browser. During the process, the device acts as an SSL client and SSL server to establish connections to the Web server and Web browser respectively. The SSL proxy certificate is generated by using the device's local certificate and re-signing the website certificate. The process is described as below:



The second scenario, the device works as the gateway of Web servers. The device with SSL proxy enabled can work as the SSL server, use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), and send the decrypted traffic to the internal Web server.

Work Mode

There are two work modes. For the first scenario, the SSL proxy function can work in the "Client Inspection - Proxy" mode ; for the second scenario, the SSL proxy function can work in the "Server Inspection - Offload" mode and "Server Inspection - Proxy" mode.

When the SSL proxy function works in the "Client Inspection - Proxy" mode, it can perform the SSL proxy on specified websites.

For the websites that do not need SSL proxy, it dynamically adds the IP address and port of the websites to a bypass list, and the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will be bypassed.

For the websites proxied by the SSL proxy function, the device will check the parameters of the SSL negotiation. When a parameter matches an item in the checklist, the corresponding HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic can be blocked or bypassed according to the action you specified.

- If the action is Block, the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will be blocked by the device.
- If the action is Bypass, the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic will not be decrypted. Meanwhile, the device will dynamically add the IP address and port number of the Website to the bypass list, and the HTTPS/POP3S/SMTPS/IMAPS traffic/RDPS/FTPS will be bypassed.

The device will decrypte the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic that are not blocked or bypassed.

When the SSL proxy function works in the "Server Inspection - Offload" mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.

When the SSL proxy function works in the "Server Inspection - Proxy" mode, it will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and re-encrypt the traffic and send it to the Web server.

You can integrate SSL proxy function with the following:

- Integrate with the application identification function. Devices can decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic encrypted using SSL by the applications and identify the application. After the application identification, you can configure the policy rule, QoS, session limit, policy-based route.

- Support unilateral SSL proxy in WebAuth. SSL client can use SSL connection during authentication stage. When authentication is completed, SSL proxy will no longer take effect, and the client and server communicate directly without SSL encryption.
- Integrate with AV, IPS, Antispam, Sandbox , Content Filter , File Filter and URL. Devices can perform the AV protection, IPS protection, Sandbox protection, Content filter , File filter, File content cilter and URL filter on the decrypted HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, can perform the File content filter, Web content, Web posting, HTTP/FTP control on the decrypted HTTPS traffic, and can perform the Email filter on the decrypted POP3S/SMTPS/IMAPS/RDPS/FTPS traffic.

Working as the Gateway of Web Clients

To implement the SSL proxy, you need to bind an SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement the SSL proxy, take the following steps:

1. Configure the corresponding parameters of SSL negotiation, including the following items: specify the PKI trust domain of the device certificates, obtain the CN value of the subject field from the website certificate, and import a device certificate to the Web browser.
2. Configure an SSL proxy profile, including the following items: choose the work mode, configure the actions to the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when its SSL negotiation matches the item in the checklist, enable the audit warning page, and so on.
3. Bind an SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic that matches the policy rule and is not blocked or bypassed by the device.

Configuring SSL Proxy Parameters

Configuring SSL proxy parameters includes the following items:

- Specify the PKI trust domain of the device certificate
- Obtain the CN value of the website certificate
- Import a device certificate to a Web browser

Specifying the PKI Trust Domain of Device Certificate

By default, the certificate of the default trust domain trust_domain_ssl_proxy_2048 will be used to generate the SSL proxy certificate with the Web server certificate together, and then system will issue the generated SSL proxy certificate to the client. You can specify another PKI trust domain in system as the trust domain of the device certificate. The specified trust domain must have a CA certificate, local certificate, and the private key of the local certificate. To specify a trust domain, take the following steps:

1. Click **Policy > SSL Proxy**.
2. At the top-right corner of the page, click **Trust Domain Configuration**.
3. Select a trust domain from the Trust domain drop-down list.
    - The trust domain of trust_domain_ssl_proxy uses RSA and the modulus size is 1024 bits.
    - The trust domain of trust_domain_ssl_proxy_2048 uses RSA and the modulus size is 2048 bits.
4. Click **OK** to save the settings.

Obtaining the CN Value

To get the CN value in the Subject field of the website certificate, take the following steps (take www.gmail.com as the example):

1. Open the Web browser (Google Chrome is used in this example), and visit https://www.g-mail.com.

2. Click the **Security Report** button () next to the URL.

3. In the pop-up dialog box, click **View certificates**.

4. In the Details tab, click **Subject**. You can view the CN value in the text box.

Importing Device Certificate to Client Browser

In the proxy process, the SSL proxy certificate will be used to replace the website certificate. However, there is no SSL proxy certificate's root certificate in the client browser, and the client cannot visit the proxy website properly. To address this problem, you have to import the root certificate (certificate of the device) to the browser.

To export the device certificate to local PC firstly, take the following steps:

1. Export the device certificate to local PC. Select **System > PKI**.

2. In the Management tab in the PKI Management dialog box, configure the options as below:

   - Trust domain: trust_domain_ssl_proxy or trust_domain_ssl_proxy_2048
   - Content: CA certificate
   - Action: Export

3. Click **OK** and select the path to save the certificate. The certificate will be saved to the specified location.

Then, import the device certificate to the client browser. Take Google Chrome as an example:

1. Open Google Chrome.

2. From the toolbar, select **Settings > Privacy and security > Security > Manage certificates** Options.

3. In the Certificates dialog box, click the **Trusted Root Certification Authorities** tab.

4. Click **Import**. Import the certificate following the Certificate Import Wizard.

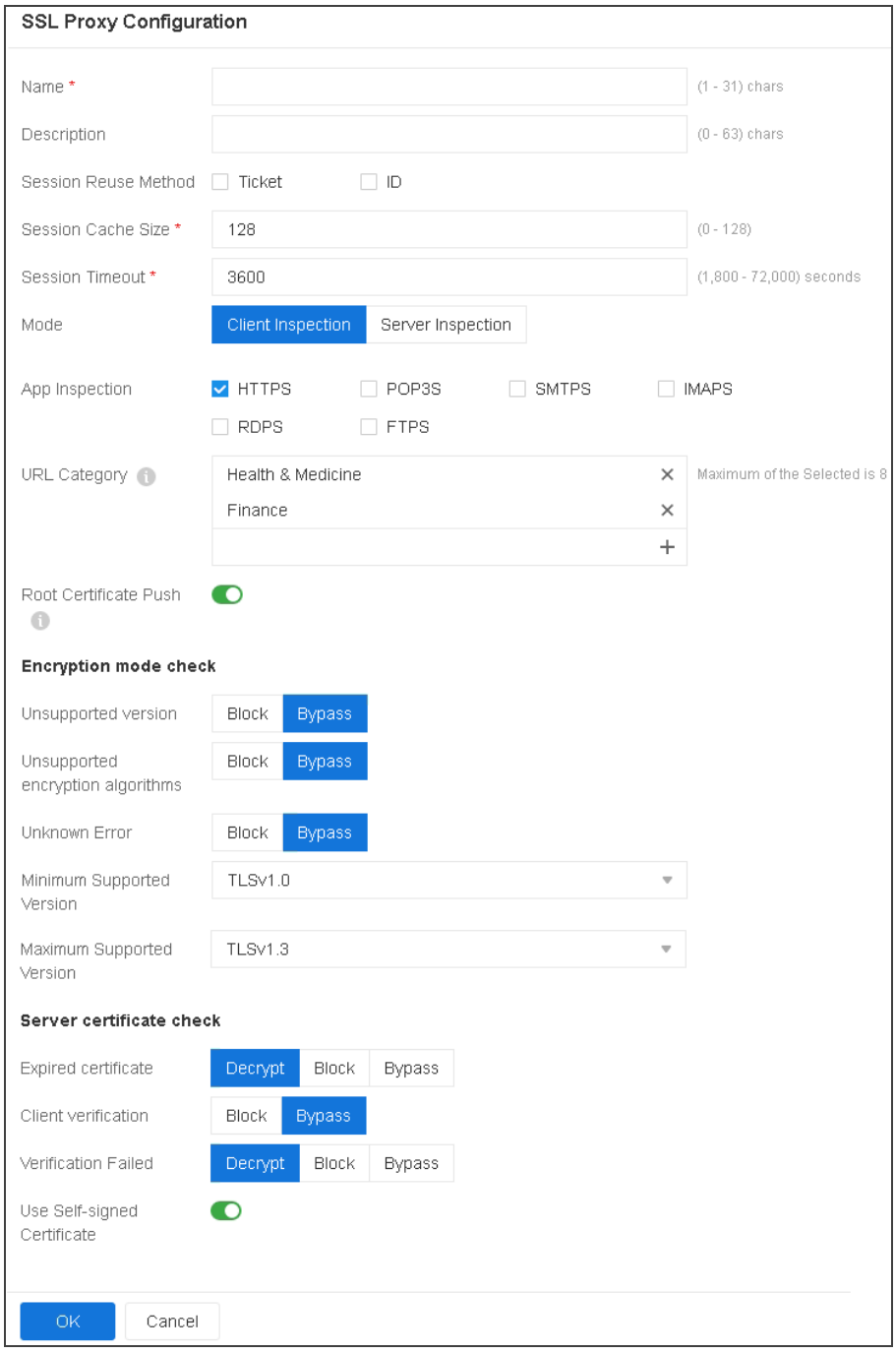
Configuring an SSL Proxy Profile

On the SSL Proxy Configuration page, you can configure the session reuse function, choose the work mode, configure the actions to the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when its SSL negotiation matches the item in the checklist, enable the audit warning page, and so forth. System supports up to 32 SSL proxy profiles.

To configure an SSL proxy profile, take the following steps:

1. Select **Object> SSL Proxy> SSL Proxy**.

2. Click **New**in the upper right corner to create a new SSL proxy profile.



In the Basic tab, configure the settings.

Option	Description
Name	Specify the name of the SSL proxy profile.
Description	Add the description of the SSL proxy file.
Session Reuse Method	After the Session Reuse function is enabled, when the client initiates an SSL connection request to the server, the server checks whether the request connection has been created, and if so, the previous SSL connection is resumed without the need for a complete TLS handshake, thereby reducing the time consumption during the handshake process. The system supports the following two session reuse methods: • Ticket: Select the check box to enable the session reuse based on session ticket. In this method, when an SSL connection is established between a client and a server for the first time, the server encapsulates the symmetric key and other status information generated in the TLS handshake into a session ticket which is encrypted, and then forwards the session ticket to the client, which is stored in the cache of the client. When the client initiates the SSL connection again (or initiates the connection request again after disconnection), the session ticket will first be sent to the server for decryption. If the server successfully decrypts and verifies the ticket, the first SSL connection will be resumed. • ID: Select the check box to enable the session reuse based on session ID. In this method, when an SSL connection is

Option	Description
	established between a client and a server for the first time, the session ID, symmetric key and other status information generated during the TLS handshake will be stored both in the cache of the client and the server. When the client initiates the SSL connection request again (or initiates the connection request again after disconnection), the server compares the session ID in the new request with the cached one and, if consistent, the first SSL connection will be resumed. **Notes:** • When the device works as the gateway of Web clients, the Web servers need to support the session reuse function. • If session reuse based on session ticket and based on session ID are both configured, session reuse based on session ticket will be prioritized.
Session Cache Size	Specifies the size of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID. **See the range and default values:**

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Model</th><th>Range (Unit: piece)</th><th>Default value (Unit: piece)</th></tr>
<tr><td>SG-6000-A1100 and below platforms of A series;</td><td>0 - 32. 0 means session cache information is not saved.</td><td>32</td></tr>
<tr><td>SG-6000-A2000 to SG-6000-A3600 of A series;</td><td>0 - 128. 0 means session cache information is not saved.</td><td>128</td></tr>
<tr><td>SG-6000-A3700 and above platforms of A series;</td><td>0-256. 0 means session cache information is not saved.</td><td>256</td></tr>
</table>
</td></tr>
<tr><td>Session Timeout</td><td>Specify the timeout value of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID. If this timeout expires, the session caches will be deleted, and when the client establishes a SSL connection with the server, it needs a complete TLS handshake. The value range is 1800 to 72000 seconds. The default value is 3600 seconds.</td></tr>
</table>

Option	Description
Mode	When the device works as the gateway of Web clients, the SSL proxy function can work in the client-inspection proxy mode. When the device works as the gateway of Web servers, the SSL proxy function can work in the server-inspection proxy/offload mode. • In the client-inspection proxy mode, the device will proxy the SSL connection from the client, decrypt and inspect its data.. • In the server-inspection proxy mode, the device will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, re-encrypt the data and send the HTTPS traffic as plaintext to the Web server. • In the server-inspection offload mode, the device will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.
App Inspec-tion	Select an application to be proxied by the SSL proxy function. Currently, system supports to perform SSL proxy on the HTTPS, POP3S, SMTPS, IMAPS, RDPS and FTPS traffic passing through the default port. By default, only the HTTPS traffic will be proxied, but you can select multiple applications as needed. To make sure the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic passing through user-defined ports will be proxied by the function, you

Option	Description
	can configure the user-defined ports in **Object > APP Book >** Static Signature Rule. **Note:** Only the predefined applications created in **Object > APP Book >** Application can be proxied by the SSL proxy function.
Root Certificate Push	Click the **Enable** button again to enable the Root Certificate Push. When the HTTPS traffic is decrypted by the SSL proxy function, the Install Root Certificate page will display in your Web browser. On the Install Root Certificate page, you can select **Download** or **Downloaded, Ignored** as needed. • Download: Click the button to download the root certificate to your local PC. For details on importing a root certificate to your Web browser, refer to Importing Device Certificate to Client Browser. • Downloaded, Ignored: If you click the button, system will no longer push the Install Root Certificate page, and will redirect you to the page you want to visit. **Notes:** • When the Install Root Certificate page appears, if you close the browser without selecting either **Download** or **Download, Ignored**, system will still push the page for your next HTTPS request. • You must install the root certificate. If you do not install the root certificate, system will prompt the access is not secure, therefore the access page may not be loaded com-

Option	Description
	pletely. Click the **Enable** button to disable the Root Certificate Push. With the function disabled, when the client initiates an HTTPS request: • If the root certificate has been installed in your Web browser, you will be redirected to the page you want to visit. • If the root certificate has not been installed in your Web browser, you will see the prompted that you're visiting is not secure.

In the Decryption Configuration tab, configure the following options. After the system completes inspection of the SSL negotiation, the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic that is not blocked or bypassed will be decrypted. If the parameters match multiple items in the checklist and you have configured different actions for different items, the Block action will take effect, and the corresponding traffic will be blocked.

Encryption mode check	
Unsupported version	Check the SSL protocol version used by the server. • When the SSL protocol used by the SSL server is not supported in system, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. The default action is to bypass the

	HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. • When the SSL protocol used by the SSL server is supported, it will continue to check other items.
Unsupported encryption algorithms	Check the encryption algorithm used by the server. • When the encryption algorithm used by the SSL server is not supported in system, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. The default action is to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. • When the encryption algorithm used by the SSL server is supported, it will continue to check other items.
Unknown Error	Check the unknown error. • When SSL negotiation fails and the cause of failure can't be confirmed, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS traffic. The default action is to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. • When system do not need check unknown failure, it will continue to check other items.
Minimum Sup-	Specify the minimum SSL protocol version supported by the sys-

ported Version	tem. When the SSL protocol version used by the SSL server meets the requirements, the system can proxy its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic.
Maximum Supported Version	Specify the minimum SSL protocol version supported by the system. When the SSL protocol version used by the SSL server meets the requirements, the system can proxy its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic.
Server certificate check	
Expired certificate	Check the certificate used by the server. When the certificate is overdue, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, or select **Decrypt** to decrypt the HTTPS/POP3S/SMTPS/IMAPS traffic. The default action is to decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic.
Client verification	Check whether the SSL server verifies the client certificate. • When the SSL server verifies the client certificate, you can select **Block** to block its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic, or select **Bypass** to bypass its HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. The default action is to bypass the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic. • When the SSL server does not verify the client certificate,

	it will continue to check other items.

Verification Failed	Verify the server certificate. You can configure an action for the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when the certificate is failed to be verified. The default action is to decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic.
	• Decrypt: Decrypt the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when the certificate is failed to be verified, and select whether to use the self-signed certificate.
	  • Use the self-signed certificate: Click the **Enable** button to use the self-signed certificate to complete the SSL negotiation with the Web browser. In this case, your browser will prompt a warning message.
	  • Do not use the self-signed certificate: Click the **Enable** button again to disable the self-signed certificate. Then, the system will use the trusted certificate "SG6000" to complete the SSL negotiation with the Web browser. If the certificate "SG6000" has been installed, your browser will not prompt a warning message.
	• Block: Block the HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when the certificate is failed to be verified.
	• Bypass: Bypass the

	HTTPS/POP3S/SMTPS/IMAPS/RDPS/FTPS traffic when the certificate is failed to be verified.

3. Click **OK** to save the settings.

Binding an SSL Proxy Profile to a Policy Rule

After binding the SSL proxy profile to a policy rule, system will process the traffic that is matched to the rule according to the profile configuration. To bind the SSL proxy profile to a policy rule, see "Security Policy" on Page 1089.

Working as the Gateway of Web Servers

To implement an SSL proxy, you need to bind an SSL proxy profile to the policy rule. After binding the SSL proxy profile to a policy rule, the system will use the SSL proxy profile to deal with the traffic that matches the policy rule. To implement SSL proxy, take the following steps:

1. Configure an SSL proxy profile. You can choose the work mode, specify the trust domain of the Web server certificate and the HTTP port number of the Web server.
2. Bind an SSL proxy profile to a proper policy rule. The device will decrypt the HTTPS traffic that matches the policy rule.

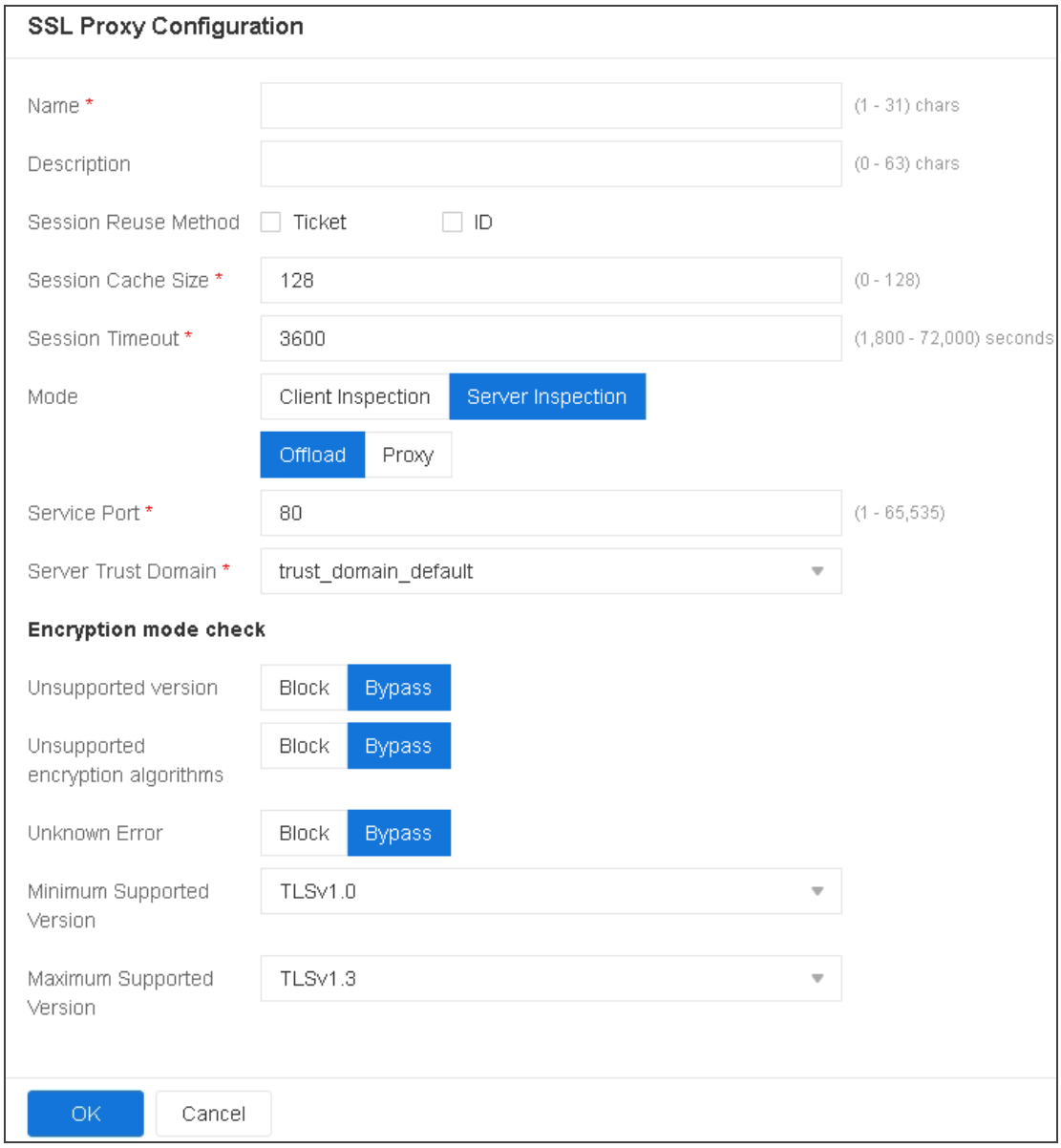
Configuring an SSL Proxy Profile

On the SSL Proxy Configuration page, you can configure options such as the session reuse, the work mode, the trust domain of the Web server certificate, and the HTTP port number of the Web server.

To configure an SSL proxy profile, take the following steps:

1. Select **Policy > SSL Proxy > SSL Proxy**.

2. Click **New** in the upper right corner to create a new SSL proxy profile.



In the Basic tab, configure the following options.

Option	Description
Name	Specify the name of the SSL proxy profile.
Description	Add the description of the SSL proxy Profile.

Option	Description
Session Reuse Method	After the Session Reuse function is enabled, when the client initiates an SSL connection request to the server, the server checks whether the request connection has been created, and if so, the previous SSL connection is resumed without the need for a complete TLS handshake, thereby reducing the time consumption during the handshake process. The system supports the following two session reuse methods: • Ticket: Select the check box to enable the session reuse based on session ticket. In this method, when an SSL connection is established between a client and a server for the first time, the server encapsulates the symmetric key and other status information generated in the TLS handshake into a session ticket which is encrypted, and then forwards the session ticket to the client, which is stored in the cache of the client. When the client initiates the SSL connection again (or initiates the connection request again after disconnection), the session ticket will first be sent to the server for decryption. If the server successfully decrypts and verifies the ticket, the first SSL connection will be resumed. • ID: Select the check box to enable the session reuse based on session ID. In this method, when an SSL connection is established between a client and a server for the first time, the session ID, symmetric key and other status inform-

Option	Description
	ation generated during the TLS handshake will be stored both in the cache of the client and the server. When the client initiates the SSL connection request again (or initiates the connection request again after disconnection), the server compares the session ID in the new request with the cached one and, if consistent, the first SSL connection will be resumed. **Notes:** • When the device works as the gateway of Web servers, the Web clients need to support the session reuse function. • If session reuse based on session ticket and based on session ID are both configured, session reuse based on session ticket will be prioritized.
Session Cache Size	Specifies the size of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID. **See the range and default values:**

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td></td><td>
<table>
<tr><th>Model</th><th>Range (Unit: piece)</th><th>Default value (Unit: piece)</th></tr>
<tr><td>SG-6000-A1100 and below platforms of A series;</td><td>0 - 32. 0 means session cache information is not saved.</td><td>32</td></tr>
<tr><td>SG-6000-A2000 to SG-6000-A3600 of A series;</td><td>0 - 128. 0 means session cache information is not saved.</td><td>128</td></tr>
<tr><td>SG-6000-A3700 and above platforms of A series;</td><td>0-256. 0 means session cache information is not saved.</td><td>256</td></tr>
</table>
</td></tr>
<tr><td>Session Timeout</td><td>Specify the timeout value of the session caches stored in the system during session reuse based on session ticket or during session reuse based on session ID. If this timeout expires, the session caches will be deleted, and when the client establishes a SSL connection with the server, it needs a complete TLS handshake. The value range is 1800 to 72000 seconds. The default value is 3600 seconds.</td></tr>
</table>

Option	Description
Mode	Select the server-inspection proxy/offload mode. When the device works as the gateway of Web servers, the SSL proxy function can work in this mode. • In the server-inspection proxy mode, the device will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, re-encrypt the data and send the HTTPS traffic as plaintext to the Web server. • In the server-inspection offload mode, the device will proxy the SSL connections initialized by Web clients, decrypt the HTTPS traffic, and send the HTTPS traffic as plaintext to the Web server.
Service Port	Specify the HTTP port number of the Web server when the device works in the server-inspection proxy/offload mode.
Server Trust Domain	Since the device will work as the SSL server and use the certificate of the Web server to establish the SSL connection with Web clients (Web browsers), you need to import the certificate and the key pair into a trust domain in the device. For more information about importing the certificate and the key pair, see "PKI" on Page 542. After you complete the importing, select the trust domain used by this SSL Profile.
Warning	Select **Enable** to enable the warning page. When the HTTPS traffic is decrypted by the SSL proxy function, the request to a HTTPS website will be redirected to a warning page of SSL proxy. In this page, system notifies the users that

Option	Description
	their access to HTTPS websites are being monitored and asks the users to protect their privacy.

3. Click **OK** to save the settings.

Binding an SSL Proxy Profile to a Policy Rule

After binding the SSL proxy profile to a policy rule, system will process the traffic that is matched to the rule according to the profile configuration. To bind the SSL proxy profile to a policy rule, see "Security Policy" on Page 1089.

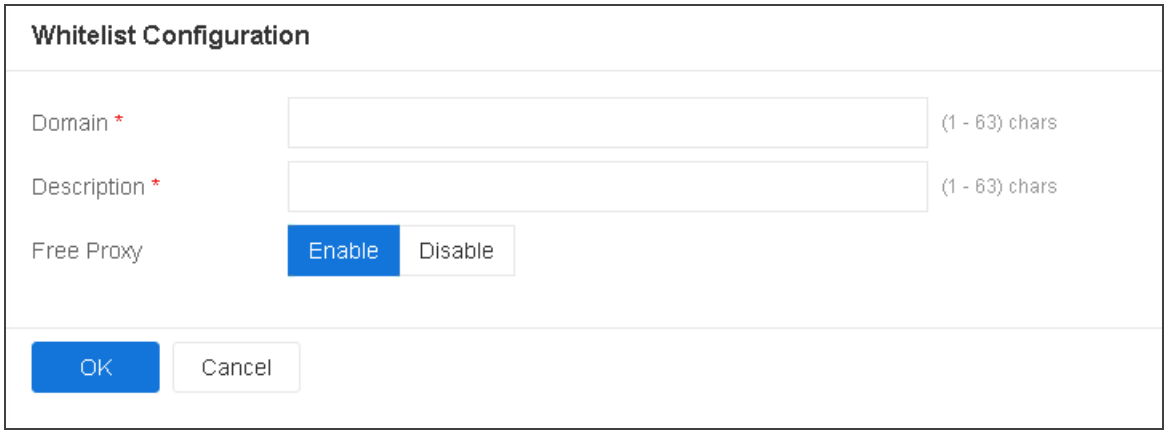
Configuring Domain White List

Websites that do not need or support SSL proxy can be added to the domain white list. The system provides the predefined domain white list to save the sites that do not support SSL proxy. For example, sites that require client certificate authentication or sites with fixed website certificates. You can also add sites to the domain white list as needed. The sites on the predefined domain white list cannot be edited or deleted.

Creating a User-defined Domain White List

If you choose not to decrypt a site out of service concerns, privacy concerns, or other voluntary reasons, you can add it to the domain white list. The device will not perform the SSL proxy function for the sites on the white list. To create a user-defined domain white list, take the following steps:

1. Select **Object > SSL Proxy > Domain White List**.
2. Click **New** to create a new domain white list.



Option	Description
Domain	Enter the domain of the domain white list. You can enter 1 to 63 characters and the domain is case sensitive. You can use the wildcard "*" in the domain. The wildcard "*" can only be used once and should be placed at the beginning of the domain, such as "*.hillstonenet.com".

Option	Description
Description	Enter the description of the user-defined domain white list. You can enter 1 to 63 characters.
Free Proxy	Click **Enable** or **Disable** button to enable or disable the domain white list.

3. Click **OK**.

Editing a User-defined Domain White List

To edit a user-defined domain white list, take the following steps:

1. Select **Object > SSL Proxy > Domain White List**.
2. On the domain white list, select the site that needs to be edited on the domain white list entry to edit and click **Edit**.
3. On the **Whitelist Configuration** page, edit the description information and the Free Proxy status of the selected site.
4. Click **OK**.

Deleting a User-defined Domain White List

To delete a user-defined domain white list, take the following steps:

1. Select **Object > SSL Proxy > Domain White List**.
2. 2. On the domain white list, select the site that needs to be deleted on the domain white list entry to delete and click **Delete**.
3. Click **Delete** in the pop-up dialog box to delete this site from the domain white list.

Exporting the Domain White List

The system exports the domain white list file in .csv format, of which the content is the real-time information of the domain white list in the system.

To export the domain white list from the system to local, take the following steps:

1. Select **Object > SSL Proxy > Domain White List**.
2. Click **Export**.

Configuring the IP Whitelist

The device will not perform the SSL proxy function for the traffic from the IPs listed on the IP whitelist. You can add the IP, the traffic from which does not need or support SSL proxy, to the IP whitelist. The IP whitelist contains dynamic IP whitelist and static IP whitelist.

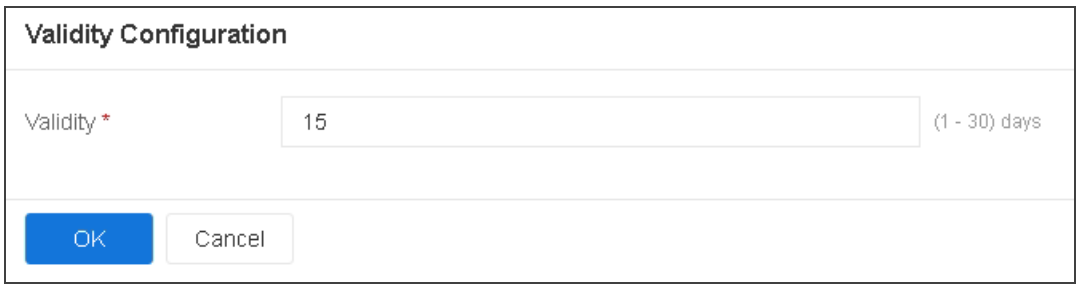
Configuring Dynamic IP Whitelist

When the device works as the gateway of Web clients, the system automatically adds the IP address to the dynamic IP whitelist in the following conditions: The traffic from this IP cannot be SSL proxied by the system and the action for this traffic is to bypass. In this scenario, the system will not perform the SSL proxy function for the traffic from the IPs listed on the IP whitelist in the future. For more information on the configuration of the SSL proxy profile, see Configuring an SSL Proxy Profile. The traffic from the IP, which is added to the dynamic IP whitelist because its traffic cannot be proxied by the device, will be re-proxied again after the validity time is due. You can configure the validity time of IPs on the dynamic IP whitelist. The system automatically deletes the existing dynamic IPs on the whitelist after their validity time is due. The system checks the dynamic IPs on the whitelist every hour to delete the IPs that expire.

Configuring the Validity Time of the Dynamic IP Whitelist

To configure the validity time of the dynamic IPs on the whitelist, take the following steps:

1. Select **Object > SSL Proxy > IP WhiteList**.
2. Click the **Validity Configuration**.



3. On the Validity Configuration page, configure the following options.

Option	Description
Validity	Specify the validity time of the dynamic IPs on the whitelist. The unit is by day. The range of the validity time is from 1 to 30 days. The default validity time is 15 days.

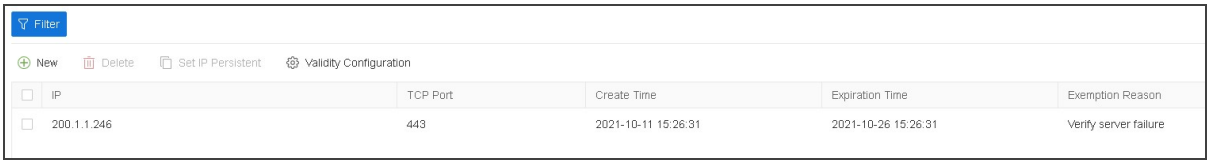
4. Click **OK**.

Notes: After you modify the SSL Profile policy or change the validity time of the dynamic IPs on the whitelist, the system deletes all current dynamic IPs on the whitelist.

Configuring the Dynamic IPs on the Whitelist to be Permanently Valid

To prevent the specified dynamic IPs on the whitelist from being automatically deleted by the system, you can configure the dynamic IP on the whitelist to be permanently valid. To configure a dynamic IP on the whitelist to be permanently valid, take the following steps:

1. Select **Object > SSL Proxy > IP WhiteList**.



2. On the IP whitelist, select the IP that needs to be set permanently valid and click **Set IP Persistent**.

3. Click **OK**.

Configuring Static IP Whitelist

The device will not perform the SSL proxy function for the traffic from the IPs on the IP whitelist. You can create a static IP on the whitelists as needed and the static IPs on the whitelist never expire. To create a static IP on the whitelist, take the following steps:

1. Select **Object > SSL Proxy > IP WhiteList**.

2. Click **New**.



3. On the IP Whitelist Configuration page, configure the following options.

Option	Description
Type	Specify the IP type of the static IP on the whitelist as IPv4 or IPv6.
IP	Specify the IP address of the static IP on the whitelist.
TCP Port	Specify the TCP port of the static IP on the whitelist. System provides 4 predefined ports: 443, 465, 993, and 995. You can choose from the dropdown box as needed, or directly enter the port number in the text box.

4. Click **OK**.

Deleting IP Whitelist

To delete the IP on the whitelist, take the following steps:

1. Select **Object > SSL Proxy > IP WhiteList**.

2. On the IP whitelist page, select the IP that needs to be deleted and click **Delete**.

3. Click **Delete** in the pop-up dialog box to delete this IP from the IP whitelists.



Notes: The total number of IPs that can be listed on the whitelist varies on different platforms. When the number of IP addresses that can be listed on the whitelist exceeds its upper limit, the system generates event logs to remind you of clearing IPs on the whitelist.

SLB Server Pool

The SLB function uses the load balancing algorithm to distribute the traffic and this utilizes the resources of the intranet servers. You can use the following methods to balance the server load:

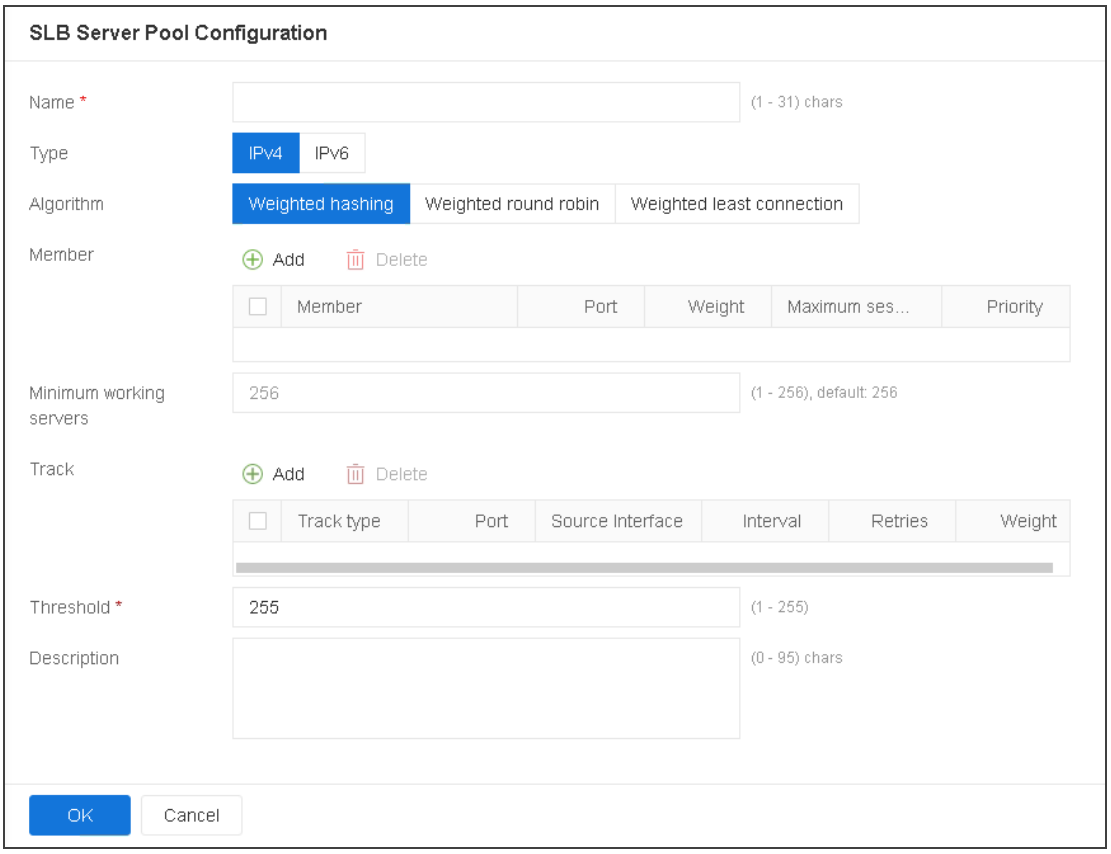
- Distribute the traffic to the specified port of each intranet server. This is applicable to the scenario that different intranet servers provide the same service via specified port at the same time.
- Distribute the traffic to different ports of an intranet server. This is applicable to the scenario that an intranet server provides the same service by running the same process at different ports.
- Combine the above two methods.

Configuring SLB Server Pool and Track Rule

To configure an SLB server pool and track rule, take the following steps:

1. Select **Object > SLB Server Pool**.

2. Click **New**. The SLB Server Pool Configuration dialog box appears.



Option	Description
Name	Specifies the name of the SLB server pool.
Type	Specifies the type of the SLB server pool, include IPv4 or IPv6.
Algorithm	Select an algorithm for load balancing, including: • Weighted Hash: Assign requests to SLB server pool members according to HASH algorithm. • Weighted Least Connection: Assign requests to the member who has the least connections in the current SLB server pool. • Weighted Round Robin: Assign requests according to

Option	Description
	weighted value of every SLB server pool members.
Member	
Member	Specifies the member of the pool. You can type the IP range or the IP address and the netmask.
Port	Specifies the port number of the server.
Maximum Sessions	Specifies the allowed maximum sessions of the server. The value ranges from 0 to 1,000,000,000. The default value is 0, which represents no limitation.
Weight	Specifies the traffic forwarding weight during the load balancing. The value ranges from 1 to 255.
Add	Add the SLB address pool member to the SLB server pool. You can add up to 256 members.
Minimum working servers	Specifies the minimum number of working servers that must work simultaneously. The value ranges from 1 to 256. The default value is 256. The system checks from high priority to low priority according to the configured minimum number of working servers. When the number of working servers within the current priority range meets the minimum requirement, the working servers within that priority range will participate in traffic distribution. If the minimum number of working servers is not met, or if the status of one of the servers becomes unreachable resulting in the number of working servers in the current priority range being less than the minimum threshold, the system will continue to check the servers in the next lower priority

Option	Description
	range until the minimum number of working servers is met.
Track	
Track Type	Selects a track type.
Port	Specifies the port number that will be tracked. The value ranges from 0 to 65535. • When the members in the SLB server pool have the same IP address and different ports, you don’ t need to specify the port when configuring the track rule. System will track each IP address and its port in the SLB server pool. • When there is a member whose port is not configured exists in the SLB sever pool, you must specify the port when configuring the track rule. System will track the specified port of the IP addresses in the SLB server pool. • When the members in the SLB server pool are all configured with IP addresses and ports and these configured IP addresses are different from each other, you can select whether to specify the port when configuring the track rule. If specified, system will track the specified port of these IP addresses. If not, system will track the configured ports of the IP addresses of the members.
Interface	Specify the source interface of the track rule. The system will use the IP address of the specified interface as the source IP address to send Ping/TCP/UDP messages.

Option	Description
Interval	Specifies the interval between each Ping/TCP/UDP packet. The unit is second. The value ranges from 3 to 255.
Retries	Specifies a retry threshold. If no response packet is received after the specified times of retries, System will determine this track entry fails, i.e., the track entry is unreachable. The value range is 1 to 255.
Weight	Specifies a weight for the overall failure of the whole track rule if this track entry fails. The value range is 1 to 255.
Add	Click **Add** to add the configured track rule to the list.
Threshold	Types the threshold for the track rule into the **Threshold** box. The value range is 1 to 255. If the sum of weights for failed entries in the track rule exceeds the threshold, system will conclude that the track rule fails.
Description	Types the description for this track rule.

3. Click **OK** to save the settings.

Viewing Details of SLB Pool Entries

To view the details of the servers in the SLB pool, take the following steps:

1. Click **Object > SLB Server Pool**.
2. Select "+" before an SLB pool entry.
3. In the Server List tab under the entry, view the information of the servers that are in this SLB pool.

4. In the Monitoring tab, view the information of the track rules.

5. In the Referenced tab, view the DNAT rules that use the SLB pool.

Schedule

System supports a schedule. This function allows a policy rule or NAT rule to take effect in a specified time and controls the duration of the connection between a PPPoE interface and the Internet. The schedule consists of a periodic schedule and an absolute schedule. The periodic schedule specifies a time point or time range for periodic schedule entries, while the absolute schedule decides a time range in which the periodic schedule will take effect.

Periodic Schedule

Periodic schedule is the collection of periods specified by all of the schedule entries within the schedule. You can add up to 16 schedule entries to a periodic schedule. These entries can be divided into 3 types:

- Daily: The specified time of every day, such as Everyday 09:00:30 to 18:00:20.
- Days: The specified time of a specified day during a week, such as Monday Tuesday Saturday 09:00:15 to 13:30:45.
- Period: A continuous period during a week, such as from Monday 09:30:30 to Wednesday 15:00:05.

Absolute Schedule

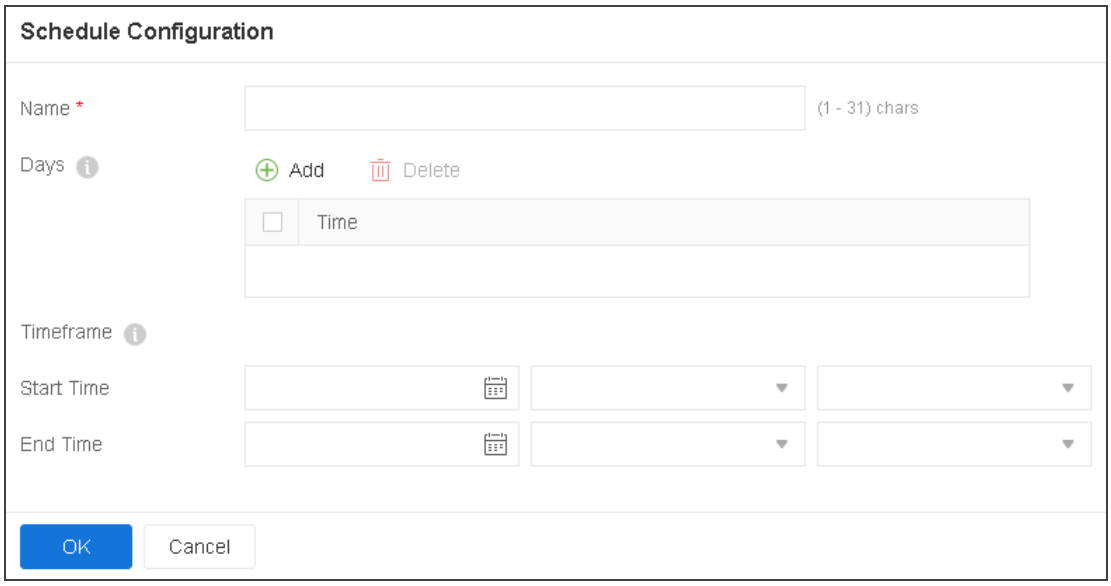
An absolute schedule is a time range in which a periodic schedule will take effect. If no absolute schedule is specified, the periodic schedule will take effect as soon as it is used by some module.

Creating a Schedule

To create a schedule, take the following steps:

1. Select **Object > Schedule**.

2. Click **New**.



Schedule Configuration Dialog Box		
Name	Specifies a name for the new schedule.	
Add	Specifies a type for the periodic schedule in Add Periodic Schedules section.	
	Type	• Daily - The specified time of every day. Click this radio button, and then, in the Time section, select a start time and end time from the Start time and End time drop-down list respectively. • Days - The specified time of a specified day during a week. Click this radio button, and then select a day/days in the Days and Time section, and finally select a start time and end

Schedule Configuration Dialog Box	
	time from the Start time and End time drop-down list respectively. • Duration - A continuous period during a week. Click this radio button, and then in the Duration section select a start day/time and end day/time from the Start time and End time drop-down list respectively. Preview Preview the detail of the configured periodic schedule in the Preview section.
Delete	Select the entry you want to delete from the period schedule list below, and click **Delete**.
Absolute Schedule	The absolute schedule decides a time range in which the periodic schedule will take effect. Without configuring an absolute schedule, the periodic schedule will take effect as soon as it is used by some module.

3. Click **OK**.

Notes: In both absolute schedule and periodic schedule, the interval between the Start time and the End time should not be less than 1 minute.

AAA Server

An AAA server is a server program that handles user requests to access computer resources, and for an enterprise, this server provides authentication, authorization, and accounting (AAA) ser-

vices. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.

Here in StoneOS system, authentication supports the following six types of AAA server:

- Local server: a local server is the firewall itself. The firewall stores user identity information and handles requests. A local server authentication is fast and cheap, but its storage space is limited by the firewall hardware size.
- External servers:
  - Radius Server
  - LDAP Server
  - Active-Directory Server
  - TACACS+ Server
  - OAuth2 Server

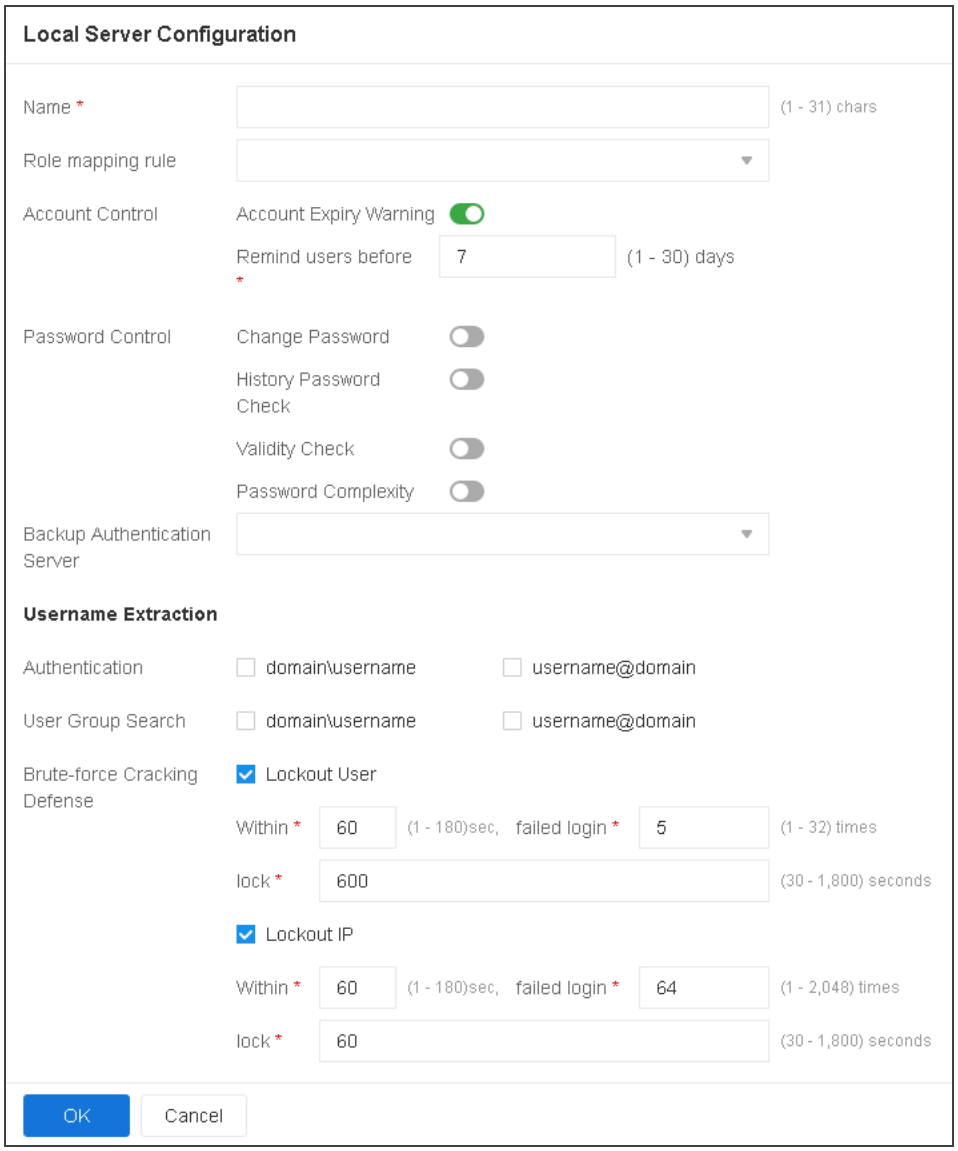
According to the type of authentication, you need to choose different AAA servers:

- : Only local and Radius servers support these authentication.
- "Configuring IPSec-XAUTH Address Pool" on Page 601: Local, Radius, Ldap, AD and Tacacs+ servers are supported.
- Other authentication methods mentioned in this guide: all four servers can support the other authentication methods.

Configuring a Local AAA Server

1. Select **Object > AAA Server**, and click **New > Local Server**.

2. The **Local Server Configuration** page opens.



Configure the following.

Option	Description
Name	Type the name for the new server into the text box.
Role mapping rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for the users who have

Option	Description
	been authenticated to the server according to the specified role mapping rule.
Account Control	To improve the account security, the system provides the account control function. • Account Expiry Warning: With this function enabled, the system checks the status of the user account on the local server, that is, checks whether the account expires. If the account is about to expire, the system sends an notification on how many days are remained before the expiration date. Account Expiry Warning is disabled by default. Click the button to enable this function. You can also specify the warning period before account expiry in the **Remind users before** textbox . The value range is from 1 to 30 days. For example, if the value is set to 10, it indicates that you will get a warning about the approaching account expiry 10 days before the expiration date. The default value is 7.  Notes: • For more information about how to configure the expiration date, refer to Creating a Local User. • In the scenario where Account

Option	Description
	 Expiry Warning is enabled and configured, Web Authentication is enabled and the authentication server is a local server, when a user whose account is about to expire attempts to login through Web authentication, the system will display a message on the Web authentication login page, warning how many days are remained before the account expiration date. • If the system uses a local authentication server for user authentication of the SSL VPN/ZTNA client, when users whose accounts are about to expire log in to the system through SSL VPN/ZTNA client, a window will pop up on the client to show the remaining number of days their account is valid. The client versions that support the pop-up

Option	Description
	 window reminder of the remaining valid days of the account include Windows client v5.0.1.10328 and later, Android client v5.0.1.10331 and later, iOS client v5.0.1 and later, macOS client v5.0.1.10331 and later, Linux client v5.0.1.10331 and later. Other client versions do not have a pop-up reminder.
Password Control	To prevent account security problem, you can configure the password control function. • Change Password: Click the button to enable the Change Password function. With this function enabled, the system allows users to change their own passwords after the successful WebAuth or SSL VPN authentication. • Change Password after First Login: Click the button to enable **Change Password after First Login**. Before enabling this function, you need to enable the **Change password** function first. With this function enabled, when you log in for web authentication for the first

Option	Description
	time, the prompt "Change the password for the first login" appears, forcing you to change the password according to the configured password complexity. When you log in to the SSL VPN for the first time, two modes are available for you: • Compatible Mode: ① If this function does not apply to the SSL VPN client, you can log in to the SSL VPN client for the first time without changing the password. ② If this function applies to the SSL VPN client, you need to change the login password immediately after logging in to the SSL VPN client for the first time. • Enforce Mode: Users need to change the login password immediately after logging in to the SSL VPN client for the first time.  Notes: • In case the Enforce Mode is configured, the SSL VPN client cannot be used if this function is not supported by the SSL VPN client. You are advised to upgrade the SSL VPN client or switch to the compatible mode.

Option	Description
	 The SSL VPN client versions that allow you to change the password upon the first login are as follows: SSL VPN Windows client 1.4.9.1274 or later version, Linux 1.4.0 or later version, Android 4.5 or later version, and iOS 2.0.6 or later version. • Change Password after First Login function is not supported by SSL VPN Windows client(non-administrator) version 1.5.x. • History Password Check: Click the button to enable **History Password Check**. With the function enabled, when you change the password, the system verifies that whether the new password is the same as historical passwords. Specify the number of historical passwords to be verified. The value rage is from 1 to 5. The default value is 3, indicating that the new password cannot be the same as the last three historical passwords. • Validity Check: Click the button to enable **Validity Check**. With this function enabled, the system checks the validity of the password. Configure the valid period

Option	Description

	of password in the textbox.
	• Password Expiry Warning: Click the button to enable **Password Expiry Warning** and configure the warning period before password expiry. The value range is from 1 to 30 days. For example, if the value is set to 10, it indicates that you will get a warning about the approaching account expiry 10 days before the expiration date. The default value is 7.
	• Password Complexity: The lower the complexity of the password, the more likely it is to be cracked. Examples of low complexity are passwords containing username or short passwords. For security reasons, you can enable the password complexity configuration and configure the password complexity requirements to ensure that the user's password has high complexity. Click the button to enable **Password Complexity** configuration.
	  • Minimum Password Length: Specifies the minimum password length. The value range is 1 to 16. The default value is 1.
	  • Minimum Capital Letter Length: Specifies the minimum length of uppercase letters contained in the password. The value range is 0-16. The default value is 0.

Option	Description
	• Minimum Lowercase Letter Length: Specifies the minimum length of lowercase letters contained in the password. The value range is 0-16. The default value is 0. • Minimum Number Length: Specifies the minimum length of the number contained in the password. The value range is 0-16. The default value is 0. • Minimum Special Character Length: Specifies the minimum length of special characters (that is, non-numeric characters) contained in the password. The value range is 0-16. The default value is 0. • Password cannot contain username: Click the button to enable**Password cannot contain username**. Passwords are not allowed to contain the username.
Backup Authentication Server	To configure a backup authentication server, select a server from the drop-down list. After configuring a backup authentication server for the local server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in

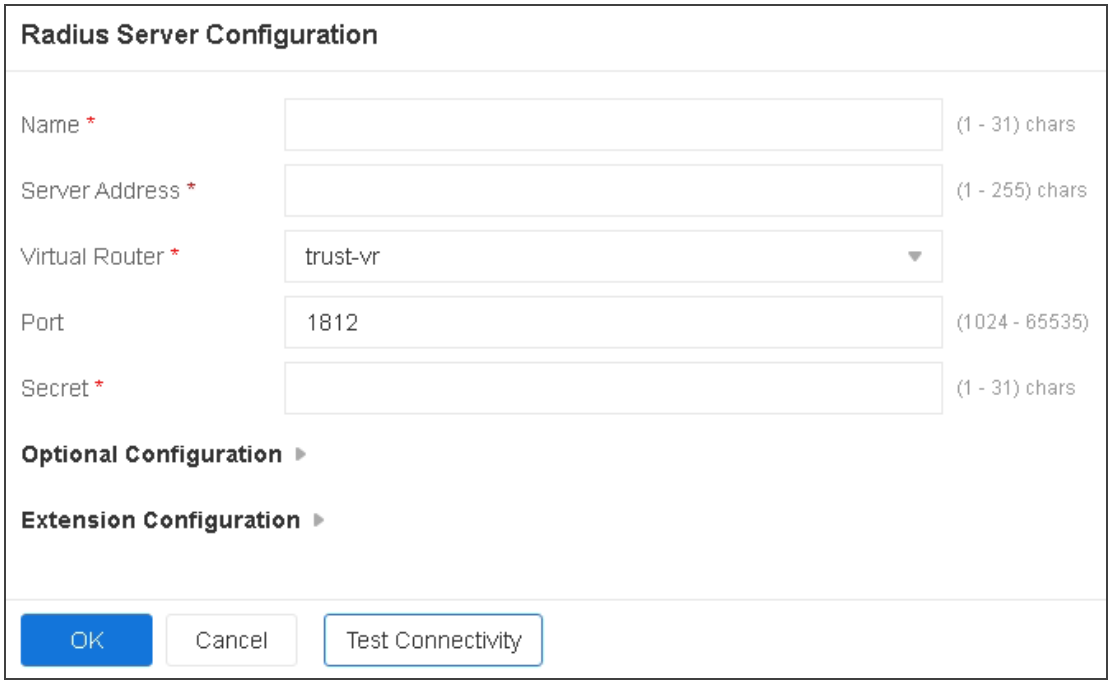
Option	Description
	system.
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available, the system will use the original user name. The supported format includes "domain\username" and "username@domain".
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name in the organization units that are locally saved. The supported format includes "domain\username" and "username@domain".
Brute-force Cracking Defense	To prevent illegal users from obtaining user name and password via brute-forth cracking, you can configure the brute-force cracking defense by locking out user or IP. • Select the **Lockout User** check box to enable the user-based brute-force cracking defense. If the failed attempts reached the specified times (1-32 times) within the specified period (1-180 seconds), the login user will be locked out for the specified time (30-1800 seconds). By default, within 60 seconds, if the failed attempts reached 5 times, the login user will be locked

Option	Description
	out for 600 seconds. • Select the **Lockout IP** check box to enable the IP-based brute-force cracking defense. If the failed attempts reached the specified times (1-2048 times) within the specified period (1-180 seconds), the IP will be locked out for the specified time (30-1800 seconds). By default, within 60 seconds, if the failed attempts reached 64 times, the IP will be locked out for 60 seconds.

3. Click **OK**.

Configuring Radius Server

1. Select **Object > AAA Server**, and click **New > Radius Server**.
2. The **Radius Sever Configuration** page opens.



Configure the following.

Basic Configuration	
Name	Specifies a name for the Radius server.
Server Address	Specifies an IP address (IPv4 or IPv6) or domain name for the Radius server.
Virtual Router	Specifies a VR for the Radius server.
Port	Specifies a port number for the Radius server. The value range is 1024 to 65535. The default value is 1812.
Secret	Specifies a secret for the Radius server. You can specify at most 31 characters.
Optional Configuration	
Authorization	When a user is authenticated by the Radius server, when the

Basic Configuration	
Policy	user is authenticated successfully, the Radius server will create a security policy for the authenticated user that includes the destination network segment, destination port, protocol, and behavior. This policy is called an authorization policy. System supports two authorization policies: "Authorization Policy During Authentication" and "Dynamic Authorization Policy". You can enable the authorization policy function to enable to obtain the authorization policy from the Radius server and add it to the system's policy list to make it effective. When the authenticated user is disconnected, the authorization policy will be deleted automatically. • By default, the authorization policy is disabled. Select the checkbox after **Authorization Policy** to enable the authorization policy. After the authorization policy of the Radius server is enabled, you add the obtained authorization policy to the aggregation policy that has been created, and arrange it as the member of aggregation policy at the end of aggregation policy, which is more convenient for the user to manage the authorization policy uniformly. If it is not added to the aggregation policy, the authorization policy will be added to the end of the system policy list by default. • Select the aggregate policy name from the drop-down list.

Basic Configuration	
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available, the system will use the original user name. The supported format includes "domain\username" and "username@domain".
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name in the organization units that are locally saved. The supported format includes "domain\username" and "username@domain".
Role mapping rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Backup server 1/ Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.
Virtual Router1/ Virtual Router2	Specifies a VR for the backup server.
Retries	Specifies a retry time for the authentication packets sent to the

Basic Configuration	
	AAA server. The value range is 1 to 10. The default value is 3.
Timeout	Specifies a timeout for the server response. The value range is 1 to 30 seconds. The default value is 3.
Backup Authentication Server	Specifies a backup authentication server. After configuring a backup authentication server for the Radius server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.
LOCAL NAS IP	Specifies the LOCAL NAS IP address. This way, the source IP address of Radius authentication packets and accounting packets, as well as the *nas-ip-address* of the authentication packets are all changed to this specified IP address, ensuring that packets returned by the Radius server are received by the current device in the complex network environment. The LOCAL NAS IP should be the same as the interface IP of the device. Otherwise, Radius authentication packets or accounting packets may not be properly sent.  Notes: • In the HA environment, the configuration of the LOCAL NAS IP address is not synchronized to the

<table>
<tr><th colspan="3">Basic Configuration</th></tr>
<tr><td></td><td colspan="2">
backup device. Therefore, you need to configure it in both primary and backup devices.
• It should be ensured that there are reachable routes between the current device and the Radius server.</td></tr>
<tr><td>Enable Accounting</td><td colspan="2">Select the Enable checkbox to enable accounting for the Radius server, and then configure options in the sliding out area.</td></tr>
<tr><td></td><td>Server Address</td><td>Specifies an IP address or domain name for the accounting server.</td></tr>
<tr><td></td><td>Virtual Router</td><td>Specifies a VR for the accounting server.</td></tr>
<tr><td></td><td>Port</td><td>Specifies a port number for the accounting server. The value range is 1024 to 65535. The default value is 1813.</td></tr>
<tr><td></td><td>Password</td><td>Specifies a password for the accounting server.</td></tr>
<tr><td></td><td>Backup server 1/Backup server 2</td><td>Specifies an IP address or domain name for backup server 1 or backup server 2.</td></tr>
<tr><td></td><td>Virtual Router-1/Virtual</td><td>Specifies a VR for the backup server.</td></tr>
</table>

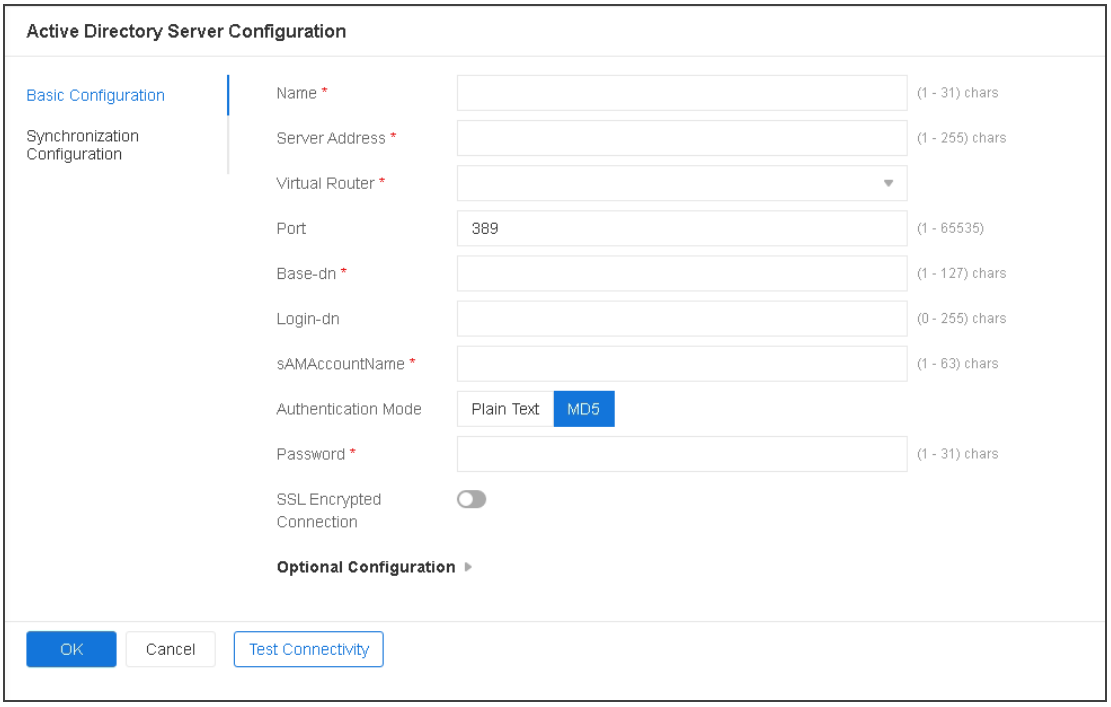
Basic Configuration		
	Router2	

3. Click **OK**.

Configuring Active Directory Server

1. Select **Object > AAA Server**, and click **New > Active Directory Server**.

2. The **Active Directory Server Configuration** page opens.



Configure the following.

Basic Configuration	
Name	Specifies a name for the Active Directory server.
Server Address	Specifies an IP address (IPv4 or IPv6) or domain name for the Active Directory server.

Basic Configuration	
Virtual Router	Specifies a VR for the Active Directory server.
Port	Specifies a port number for the Active Directory server. The value range is 1 to 65535. The default value is 389.
Base-dn	Specifies a Base-dn for the AD server. The Base-dn is the starting point at which your search will begin when the AD server receives an authentication request. For the example of abc.xyz.com as described above, the format for the Base-dn is "dc=abc,dc=xyz,dc=com".
Login-dn	Specifies authentication characteristics for the Login-dn (typically a user account with query privilege pre-defined by the AD server). When the authentication mode is plain, the Login-dn should be configured. DN (Distinguished name) is a username of the AD server who has a privilege to read user information. The format of the DN is"cn=xxx, DC=xxx,...". For example, the server domain is abc.xyz.com, and the AD server admin name is administrator who locates in Users directory. Then the login-dn should be "cn=administrator,cn=users,dc=abc,dc=xyz,dc=com".
sAMAccountName	When the authentication mode is MD5, the sAMAccountName should be configured. sAMAccountName is a username of the AD server who has a privilege to read user information. The format of sAMAccountName is "xxx". For example, the AD server admin name is admin-

Basic Configuration	
	istrator , and then the sAMAccountName should be "administrator".
Authentication Mode	Specifies an authentication or synchronization method (either plain text or MD5). The default method is MD5. If the sAMAccountName is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating the user.
Password	Specifies a password for the AD server.
SSL Encrypted Connection	Click the **Enable** button to enable the SSL encrypted connection function. With this function enabled, the system connects to the Active Directory authentication server through SSL.
Change Password	When you edit the configuration of the server, you can enable this function, enter a new password in the field, and then save the configuration.
Optional Configuration	
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available,

Basic Configuration	
	the system will use the original user name. The supported format includes "domain\username" and "user-name@domain".
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name in the organization units that are locally saved. The supported format includes "domain\username" and "username@domain".
Role Mapping Rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for users who have been authenticated to the server according to the specified role mapping rule.
Backup server 1/Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.
Virtual Router-1/Virtual Router2	Specifies a VR for the backup server.
Authentication Base-DN	Specifies an authentication Base-dn for the AD server. All users in the Base-DN (including those directly under the user group) will be allowed to pass the authentication. The format of the DN is"OU=xxx, DC=xxx,...".
Backup Authentication Server	Specifies a backup authentication server. After configuring a backup authentication server for the Active Dir-

Basic Configuration	
	ectory server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.
Brute-force Cracking Defense	To prevent illegal users from obtaining user name and password via brute-forth cracking, you can configure the brute-force cracking defense by locking out user or IP. • Select the **Lockout User** check box to enable the user-based brute-force cracking defense. If the failed attempts reached the specified times (1-32 times) within the specified period (1-180 seconds), the login user will be locked out for the specified time (30-1800 seconds). By default, within 60 seconds, if the failed attempts reached 5 times, the login user will be locked out for 600 seconds. • Select the **Lockout IP** check box to enable the IP-based brute-force cracking defense. If the failed attempts reached the specified times (1-2048 times) within the specified period (1-180 seconds), the IP will be locked out for the specified time (30-1800 seconds). By default, within 60 seconds, if the

Basic Configuration	
	failed attempts reached 64 times, the IP will be locked out for 60 seconds.
Mobile Attribute	Specifies the mobile number attribute name of the user. By default, mobile is used. The system can obtain the mobile number of the user by using this attribute. The mobile number is used in the SMS-based authentication scenario. For example, in the SSL VPN SMS-based authentication scenario, the system can obtain the mobile number of the user by using this attribute. When the user logs in to SSL VPN, the system will send the SMS verification code to the mobile number.
Email Attribute	Specifies the email attribute number of the user. By default, mail is used. The system can obtain the email address of the user by using this attribute. The email address is used in the email-based authentication scenario. For example, in the SSL VPN email-based authentication scenario, the system can obtain the email address of the user by using this attribute. When the user logs in to SSL VPN, the system will send the verification code to the email address.

Click Synchronization Configuration. In the tips message that appears, click OK and start the synchronization configuration.

Option	Description
Synchronization	Click the button to enable the synchronization function and

Option	Description
	you can specify the auto synchronization mode. If you disable this function, the system will stop synchronizing and clear the existing user information. By default, system will synchronize the user information on the configured authentication server with the local server every 30 minutes.
Auto Synchronization	Specifies the automatic synchronization. Interval Synchronization: Specifies the time interval for automatic synchronization. The value range is 15 to 1440 minutes. The default value is 30. Daily Synchronization: Specifies the time when the user information is synchronized everyday. The format is HH:MM, HH and MM indicates hour and minute respectively. Once Synchronization: If this parameter is specified, system will synchronize automatically when the configuration of Active-Directory server is modified. After executing this command , system will synchronize the user information immediately.
Synchronous Operation Mode	Specifies user synchronization mode, including Group Synchronization and OU Synchronization. By default, the user information will be synchronized with the local server based on the group.
Synchronous	Filter the synchronization information obtained and retain the information of the specified object. You can select the

Option	Description
Object	syn object as users or user groups. By default, users and user groups are both selected.
OU maximum depth	Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12. OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level (including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized with the local server.
Naming Attribute	Specifies the value of the username attribute. The string is usually cn (Common Name), name, or sAMAccountName. By default, sAMAccountName is used. When the system synchronizes user information to the local server, the system can obtain the username by using this attribute; When the system performs user authentication, the system can identify the user by using this attribute.
User Class	Specifies the value of objectClass of the user. By default, person is used. When the system synchronizes Active Directory user information to the local server, the system will filter user information based on user class. The system allows you to configure at most 8 user classes and the logical operator among them is OR. In other words, user information that meets at least one user class can be synchronized to the sys-

Option	Description
	tem.
Group Class	Specifies the value of objectClass of the user group. By default, group is used. When the system synchronizes Active Directory user information to the local server, the system will filter user information based on group class. The system allows you to configure at most 8 group classes and the logical operator among them is OR. In other words, user information that meets at least one group class can be synchronized to the system.
User Filter	Specifies the user-filter conditions. System can only synchronize or authenticate users that are in accordance with the filtering condition on the authentication server. The length is 0 to 120 characters. For example, if the condition is configured to “memberOf=CN=Admin,DC=test,DC=com”, system only can synchronize or authenticate user whose DN is “CN=Admin,DC=test,DC=com”. The commonly used operators are: =(equals a value)、&(and) 、|(or)、!(not)、*(Wildcard: when matching zero or more characters)、～=(fuzzy query.)、>=Be greater than or equal to a specified value in lexicographical order.)、<=(Be less than or equal to a specified value in lexicographical order.).
Synchronization Base-dn	Synchronization Base-DN is the starting point at which the system synchronizes users and user groups from the Active Directory server. Click this field. In the **Server Directory**

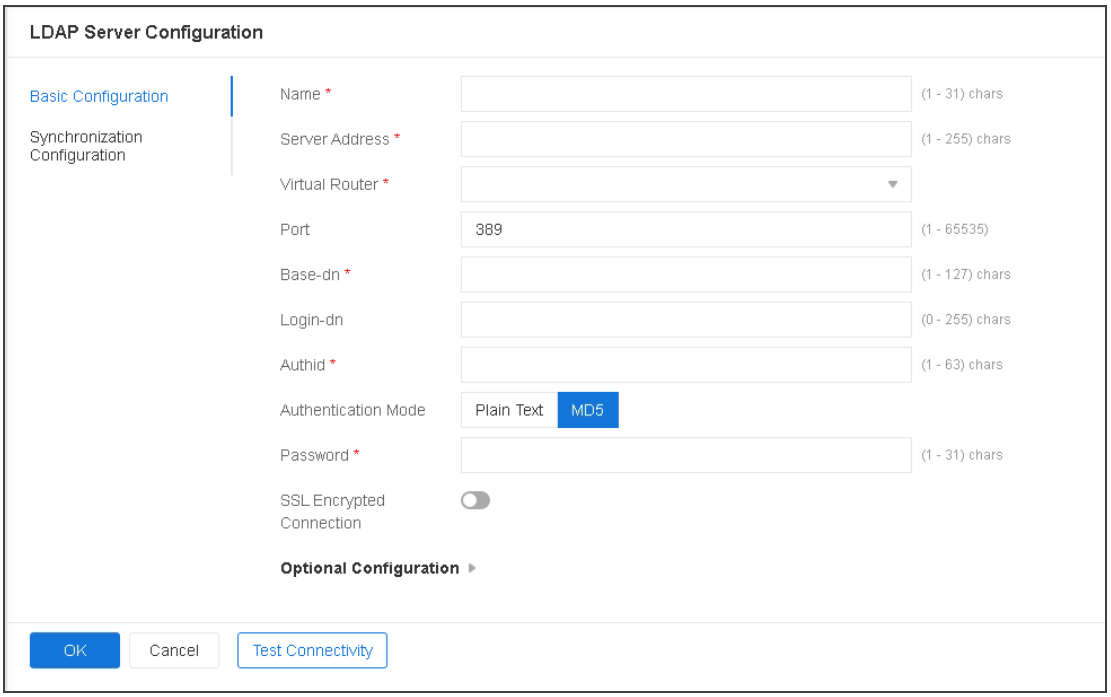
Option	Description
	panel, select the path that you want to synchronize. This way, all users and user groups in the path are synchronized to the local. At most 32 paths can be selected.

3. Click **OK**.

Configuring LDAP Server

1. Select **Object > AAA Server**, and click **New > LDAP Server**.

2. The **LDAP Server Configuration** page opens.



Configure the following

Basic Configuration	
Server Name	Specifies a name for the LDAP server.

Basic Configuration	
Server Address	Specifies an IP address (IPv4 or IPv6) or domain name for the LDAP server.
Virtual Router	Specifies a VR for the LDAP server.
Port	Specifies a port number for the LDAP server. The value range is 1 to 65535. The default value is 389.
Base-dn	Specifies the details for the Base-dn. The Base-dn is the starting point at which your search will begin when the LDAP server receives an authentication request.
Login-dn	Specifies authentication characteristics for the Login-dn (typically a user account with query privileges pre-defined by the LDAP server).
Authid	Specifies the Authid, which is a string of 1 to 63 characters and is case sensitive.
Authentication Mode	Specifies an authentication or synchronization method (either plain text or MD5). The default method is MD5. If the Authid is not configured after you specify the MD5 method, the plain method will be used in the process of synchronizing user from the server, and the MD5 method will be used in the process of authenticating user.
Password	Specifies a password for the LDAP server. This should correspond to the password for Admin DN.
SSL Encrypted Connection	Click the **Enable** button to enable the SSL encrypted connection function. With this function enabled, the system con-

Basic Configuration	
	nects to the LDAP authentication server through SSL.
Optional Configuration	
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available, the system will use the original user name. The supported format includes "domain\username" and "username@domain".
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name in the organization units that are locally saved. The supported format includes "domain\username" and "username@domain".
Role Mapping Rule	Specifies a role mapping rule for the server. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Backup server 1/Backup server 2	Specifies an IP address or domain name for backup server 1 or backup server 2.
Virtual Router-	Specifies a VR for the backup server.

Basic Configuration	
1/Virtual Router2	
Authentication Base-DN	Specifies an authentication Base-dn for the AD server. All users in the Base-DN (including those directly under the user group) will be allowed to pass the authentication. The format of the DN is"OU=xxx, DC=xxx,...".
Synchronization Base-DN	Specifies a Synchronization Base-dn for the AD server. All users and user groups in the Base-DN will be synchronized to the local. The format of the DN is"OU=xxx, DC=xxx,...".
Synchronization	Check the checkbox to enable the synchronization function; clear the checkbox to disable the synchronization function, and system will stop synchronizing and clear the existing user information. By default, system will synchronize the user information on the configured LDAP server with the local every 30 minutes.
Automatic Synchronization	Click the radio button to specify the automatic synchronization. Interval Synchronization: Specifies the time interval for automatic synchronization. The value range is 15 to 1440 minutes. The default value is 30. Daily Synchronization: Specifies the time when the user information is synchronized everyday. The format is HH:MM, HH and MM indicates

Basic Configuration	
	hour and minute respectively. Once Synchronization: If this parameter is specified, system will synchronize automatically when the configuration of LDAP server is modified. After executing this command , system will synchronize user information immediately.
Synchronous Operation Mode	Specifies the user synchronization mode, including Group Synchronization and OU Synchronization. By default, the user information will be synchronized with the local server based on the group.
Synchronization Object	Filter the synchronization information obtained and retain the information of the specified object. You can select the syn object as users or groups. By default, users and groups are both selected.
OU maximum depth	Specifies the maximum depth of OU to be synchronized. The value range is 1 to 12, and the default value is 12. OU structure that exceeds the maximum depth will not be synchronized, but users that exceed the maximum depth will be synchronized to the specified deepest OU where they belong to. If the total characters of the OU name for each level (including the "OU=" string and punctuation) is more than 128, OU information that exceeds the length will not be synchronized with the local server.

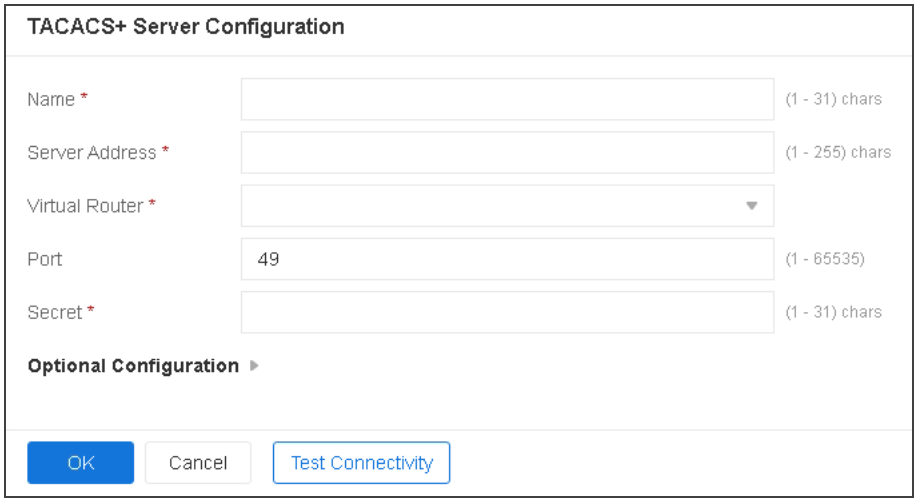
Basic Configuration	
User Filter	Specifies the user filters. System can only synchronize and authenticate users that match the filters on the authentication server. The length is 0 to 120 characters. For example, if the condition is configured to “(|(objectclass=inetOrgperson)(objectclass=person))”, system only can synchronize or authenticate users which are defined as inetOrgperson or person. The commonly used operators are as follows: =(equals a value)、&(and) 、|(or)、!(not)、*(Wildcard: when matching zero or more characters)、~=(fuzzy query.)、>=(Be greater than or equal to a specified value in lexicographical order.)、<=(Be less than or equal to a specified value in lexicographical order.).
Naming Attribute	Specifies a naming attribute for the LDAP server. The default naming attribute is uid.
Group Naming Attribute	Specifies a naming attribute of group for the LDAP server. The default naming attribute is uid.
Member Attribute	Specifies a member attribute for the LDAP server. The default member attribute is uniqueMember.
Group Class	Specifies a group class for the LDAP server. The default class is groupofuniquenames.
Backup Authentication Server	Specifies a backup authentication server. After configuring a backup authentication server for the LDAP server, the backup authentication server will take over the authen-

Basic Configuration	
	tication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.
Synchronization Base-dn	Synchronization Base-DN is the starting point at which the system synchronizes users and user groups from the LDAP server. Click this field. In the **Server Directory** panel, select the path that you want to synchronize. This way, all users and user groups in the path are synchronized to the local. At most 32 paths can be selected.

3. Click **OK**.

Configuring TACACS+ Server

1. Select **Object > AAA Server**.
2. Click **New > TACACS+ Server**, and the **TACACS+ Server Configuration** page opens.



Configure the following.

Basic Configuration	
Server Name	Enter a name for the TACACS+ server.
Server Address	Specify the IPv4 address, IPv6 address, or domain name for the TACACS+ server.
Virtual Router	Specify the VRouter of TACACS+ server.
Port	Enter port number for the TACACS+ server. The default value is 49. The value range is 1 to 65535.
Secret	Enter the shared secret to connect the TACACS+ server.
Optional	
Username Extraction	
Authentication	Specifies the authentication user name format. During authentication, the system will extract the user name for authentication based on the configured authentication user name format. If the specified format is not available, the system will use the original user name. The supported format includes "domain\username" and "username@domain".
Search Group	Specifies the user name format when the system searches from the local storage. When implementing policy control based on user name or user groups, the system will search for the group of a user name in the organization units that are locally saved. The supported format includes "domain\username" and "username@domain".
Role mapping rule	Select a role mapping rule for the server. With this option selected, system will allocate a role for the users who have

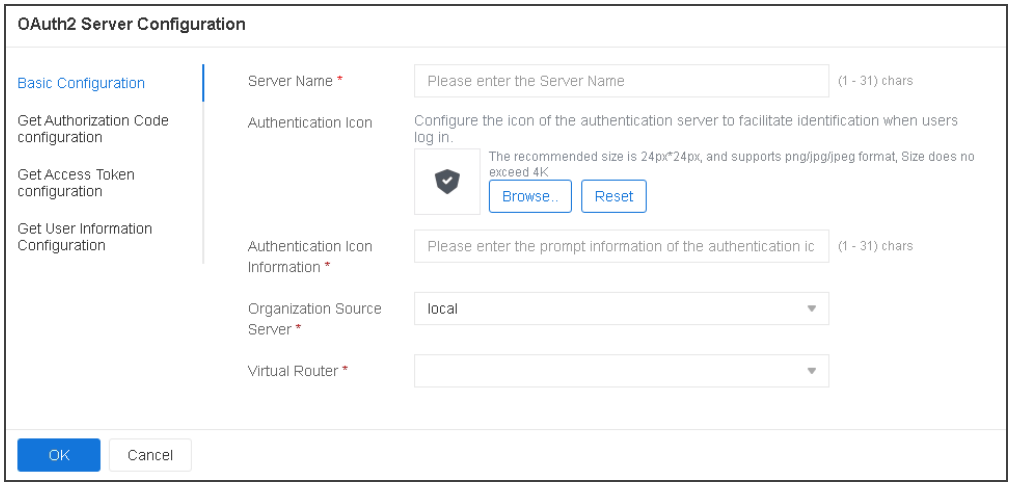
Basic Configuration	
	been authenticated to the server according to the specified role mapping rule.
Backup Server 1 (2)	Enter the IPv4 address, IPv6 address, or domain name for the backup TACACS+ server 1(or 2). The types of backup server and primary server are the same, which are TACACS+ servers. When the authentication fails via the primary server, the authentication is performed by using the backup server 1 and 2 in sequence.
Virtual Router 1 (2)	Select the VRouter for the backup server.

Configuring an OAuth2 Server

OAuth 2.0 is an authorization protocol. OAuth2 defines four grant types: authorization code, implicit, resource owner password credentials, and client credentials. The system supports only the authorization code mode. The system can request authorization codes, access tokens, and user information from the OAuth2 authorization server to implement user authentication.

1. Select **Object** > **AAA Server**.

2. Click **New** > **OAuth2 Server**.



On the OAuth2 Server Configuration page, configure the following options:

Basic Configuration	
Server Name	Enter the name of the OAuth2 authorization server.
Authentication Icon	Specifies the icon of the authorization server, which is used to be displayed on the user authentication page. To do this, click **Browse** and select an icon from your PC. To restore to the default settings, click **Reset**.
Authentication Icon Information	Specifies the prompt message of the icon. This prompt message will be displayed when you hover your mouse over the icon on the user authentication page. Example: Use Hillstone User Center for authentication.
Organization Source Server	Select the AAA server to which the authenticated user belongs from the drop-down list. A configured local, AD, or LDAP server can be selected. After you select an AAA server,

Basic Configuration	
	the system can query the user group and role information corresponding to the username of the online user on the referenced AAA server. This can implement policy control based on user group and role.
Virtual Router	Specifies the VRouter to which the OAuth2 server belongs.
Get Authorization Code Configuration	
Authorization Code Request URL	Specifies the URL of the authorization server from which the system requests an authorization code. Example: https://-passport.hillsonenet.com/OAuth/Authorize.
Request Parameter	Specifies the request parameter used for the system to apply for the authorization code, including the parameter name and parameter values. The client_id, redirect_uri, and response_type parameters are required. You can configure at most 16 request parameters. • client_id: Enter the client ID, which is obtained by the system from registration with the OAuth2 authorization server. • redirect_uri: Enter the system address to which the server redirects after authorization, provided by the system during registration with the OAuth2 authorization server. This address is listened by the system. The redirect URL is in the following format: https://*host*:17443/login/oauth (HTTPS listener) or

Basic Configuration	
	http://*host*:17080/login/oauth (HTTP listener). • response_type: Enter the response type of the authorization code request, which is fixed to "code" in authorization code mode. • Custom Parameter: Click **New** to add a custom request parameter, such as scope and display. To delete a custom request parameter, select the request parameter and click **Delete**.
Response Parameter	Specifies the parsed parameter and local variable. In authorization code mode, the parsed parameter is fixed to "code", which is stored in the local variable "$code". After the authorization code request succeeds, the system needs to parse the specified attribute field in the response and store it to the local variable for the next access token request.
Get Access Token Configuration	
Access Token Request URL	Specifies the URL of the authorization server from which the system requests an access token. Example: https://-passort.hillstonenet.com/OAuth/Token.
Request Parameter	Specifies the request parameter used for the system to apply for the access token, including the parameter name, parameter value, and parameter type. The code, redirect_uri, and grant_type parameters are required. The HTTP DATA type indicates the request content and the HTTP HEADER type indicates the request header. You can con-

Basic Configuration	
	figure at most 16 request parameters. • code: Enter the authorization code generated by the authorization server after authorization, which is fixed to "$code" in authorization code mode. Type is HTTP DATA. • redirect_uri: Enter the system address to which the server redirects after authorization, provided by the system during registration with the OAuth2 authorization server. This address is listened by the system. The redirect URL is in the following format: https://*host*:17443/login/oauth (HTTPS listener) or http://*host*:17080/login/oauth (HTTP listener). This redirect URL needs to be consistent with that requested by the authorization code. Type is HTTP DATA. • grant_type: Enter the grant type of the authorization server, which is fixed to "authorization_code" in authorization code mode. Type is HTTP DATA. • Custom Parameter: Click **New** to add a custom request parameter, such as scope and display. To delete a custom request parameter, select the request parameter and click **Delete**.
Response Parameter	Specifies the parsed parameter and local variable. In authorization code mode, the parsed parameter is fixed to "access_token", which is stored in the local variable "$access_token".

Basic Configuration	
	After the access token request succeeds, the system needs to parse the specified attribute field in the response and store it to the local variable for the next user information request.
Get User Information Configuration	
User Information Request URL	Specifies the URL of the authorization server from which the system requests user information. Example: https://passport.hillstonenet.com/API/Resource/UserInfo.
Request Parameter	Specifies the request parameter used for the system to apply for user information, including the request name, parameter value, and parameter type. The HTTP DATA type indicates the request content and the HTTP HEADER type indicates the request header. You can configure at most 16 request parameters. • New: Click **New** to add a request parameter. Example: Name: Authorization; Value: Bearer $access_token, which is the access token obtained from the previous step; Type: HTTP HEADER. • Delete: To delete a request parameter, select the request parameter and click **Delete**.
Response Parameter	Specifies the parsed parameter and local variable. In authorization code mode, the parsed parameter can be username and mail, which is stored in the local variable "$username". After the user information request succeeds, the system needs to

Basic Configuration	
	parse the specified attribute field in the response and store it to the local variable. This field is used to display the username of the authenticated user.



Notes:

- Only one OAuth2 server can be configured within each VSYS.
- The OAuth2 server that can be connected to the system includes Hillstone User Center and AzureAD.

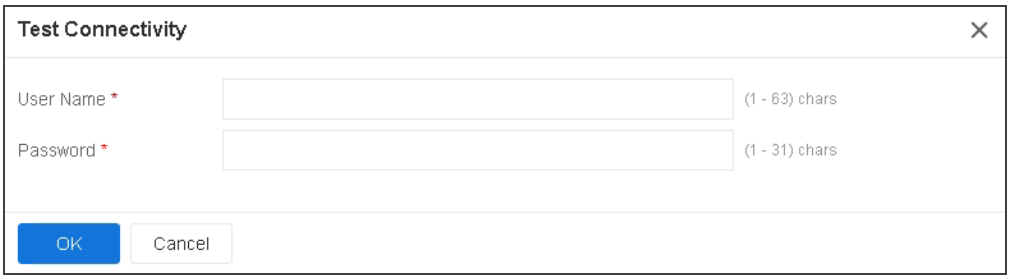
Connectivity Test

When AAA server parameters are configured, you can test if they are correct by testing server connectivity.

To test server connectivity, take the following steps:

1. Select **Object > AAA Server**, and click **New**.
2. Select your AAA server type, which can be Radius, AD, LDAP or TACACS+. The local server does not need the connectivity test.
3. After filling out the fields, click **Test Connectivity**.
4. For Radius or TACACS+ server, enter a username and password in the popped <Test Connectivity> dialog box. If the server is AD or LDAP, the login-dn and secret is used to test

connectivity.



5. Click **Test Connectivity**. If "Test connectivity success" message appears, the AAA server settings are correct.

If there is an error message, here are the causes:

- Connect AAA server timeout: Wrong server address, port or virtual router.
- AAA server configuration error: Secret is wrong.
- Wrong name or password: Username or password for testing is wrong.

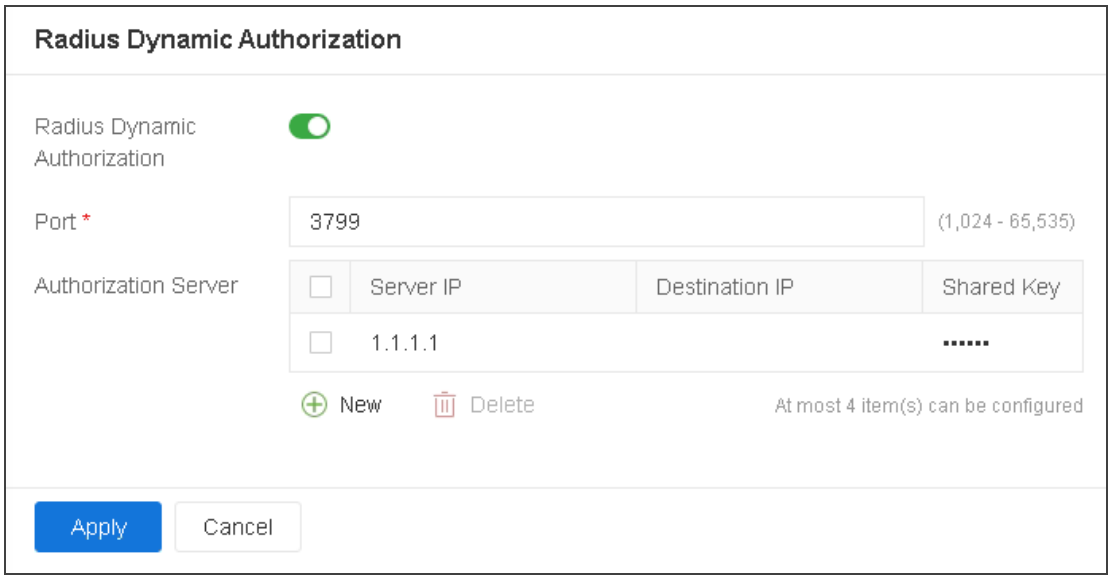
Radius Dynamic Authorization

The Radius dynamic authorization function, includes:

- When the user is authenticated successfully, the Radius server can send a Radius CoA (Change of Authorization) request message to the authority of the authenticated user to the device. The device automatically generates the security policy rule for the user. When the user goes offline, the device delete this user's security policy rule automatically
- When the SSL VPN user is authenticated successfully, the Radius server can send a Radius DM (Disconnect Messages) request message to send the accounting user information (including the user name, user IP address, user accounting ID, etc.) to the device, and the device can disconnect the specified scvpn authentication user and end the accounting.

To configure the Radius dynamic authorization function, take the following steps:

1. Select **Object** > **Radius Dynamic Authorization**.



2. Click the **Enable** button after **Radius Dynamic Authorization** to enable the Radius dynamic authorization function.

3. Type the port number of the Radius dynamic authorization server into the **Port** textbox. The value range is 1024 to 65535. The default value is 3799.

4. In the Authorization Server section, click **New**, and then specify the IP address, destination IP and shared key of the Radius dynamic authorization server.

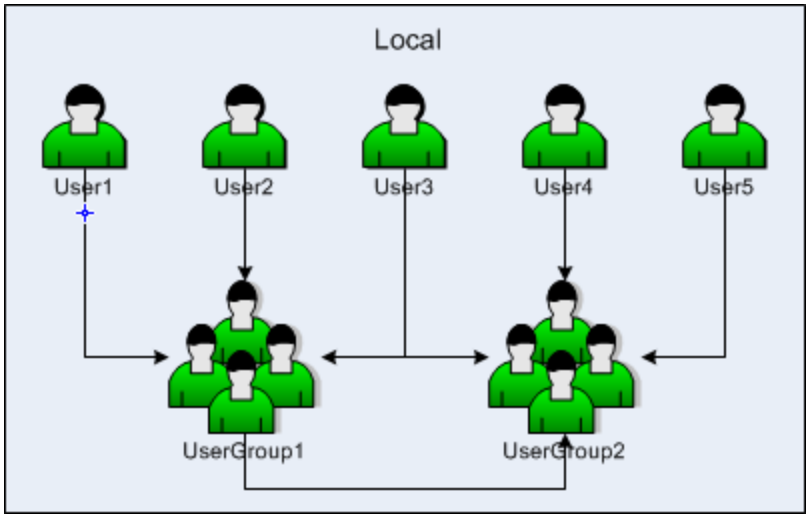
5. To delete the Radius dynamic authorization server, select the checkbox in the list, and then click **Delete**.

6. Click **Apply**.

Notes: If you need to use the Radius dynamic authorization function, first enable and configure the Radius accounting server. For the configuration, refer to Enable Accounting.

User

User refers to the user who uses the functions and services provided by the Hillstone device, or who is authenticated or managed by the device. The authenticated users consist of local user and external user. The local users are created by administrators. They belong to different local authentication servers, and are stored in system's configuration files. The external users are stored in external servers, such as AD server or LDAP server. System supports User Group to facilitate user management. Users belonging to one local authentication server can be allocated to different user groups, while one single user can belong to different user groups simultaneously; similarly, user groups belonging to one local authentication server can be allocated to different user groups, while one single user group can belong to different user groups simultaneously. The following diagram uses the default AAA server, Local, as an example and shows the relationship between users and user groups:



As shown above, User1, User2 and User3 belong to UserGroup1, while User3 also belongs to UserGroup2, and UserGroup2 also contains User4, User5 and UserGroup1.

Configuring a Local User

This section describes how to configure a local user and user group.

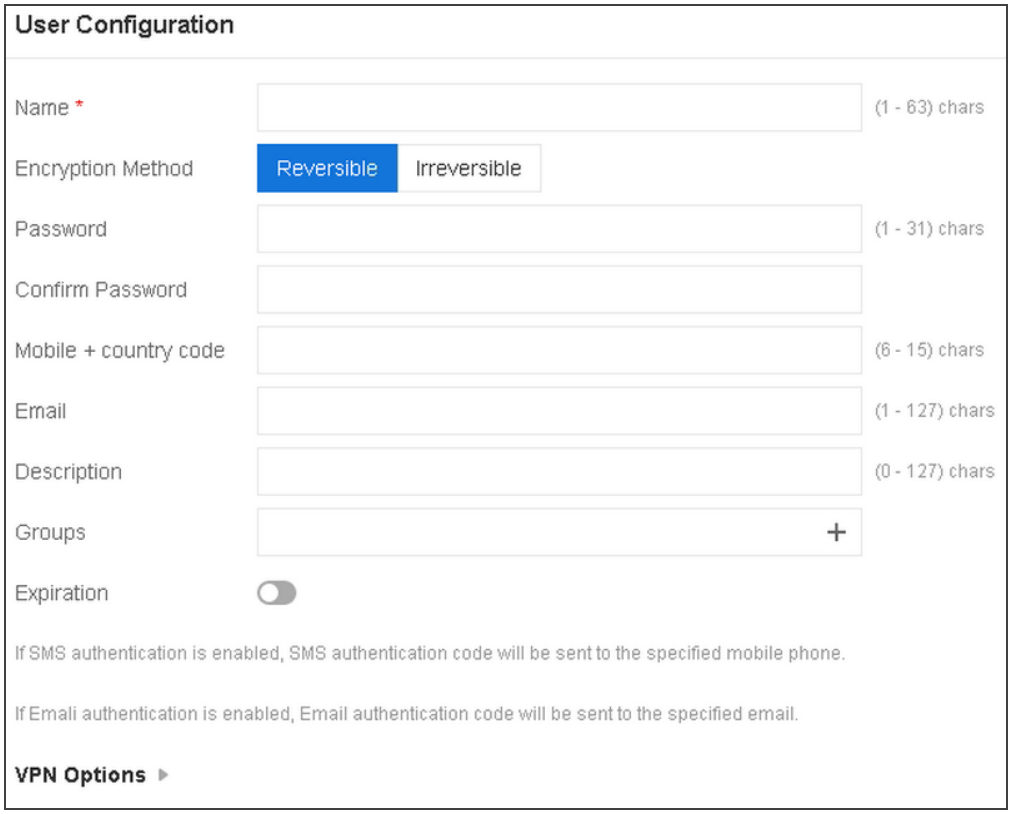
Click **Object > User > Local User** or **ZTNA > User > Local User**, some information and operations are provided as below:

- Click the "Local server" drop-down box in the upper left corner of the page to switch the local user's server.
- Red Expired, orange Will expire within a week and yellow Will expire within a month colors are used to mark the expired users , expired within a week, expired within a month in the list.
- Check the information of the local user in the list, including user, user group, expiration, mobile and description.

Creating a Local User

To create a local user, take the following steps:

1. Select **Object > User > Local User** or **ZTNA > User > Local User**.
2. Click **New > User**.



Configure the following.

Option	Description
Name	Specifies a name for the user.
Encryption Method	Specifies method to encrypt the user's password, that is, the encrypted algorithm of password is reversible or irreversible . • Reversible: System will use the reversible encryption algorithm AES to encrypt the user password. In some authentication scenarios, system can decrypt the password for authentication. • Irreversible: System will use the SHA irreversible encryption algorithm to encrypt user passwords. The

Option	Description
	passwords cannot be decrypted. In this case, the user can not authenticate through CHAP (Challenge Handshake Authentication Protocol, which is used in L2TP VPN and 802.1X).
Password	Specifies a password for the user.
Confirm password	Type the password again to confirm.
Mobile+country code	Specifies the user's mobile number. When users log into the SSL VPN client, system will send the verification code to the mobile number.
Email	Specifies the user's Email address. The value range is 1 to 127 characters. If the Email authentication function is enabled, users will receive the verification code via this Email. For more information about Email authentication, see Configuring an SSL VPN.
Description	If needed, type the description of the user.
Group	Add the user to a selected user group. Click + and the **User Group** list appears. Then, click the user group you want to add to. Note: When a user is added to more than 256 groups, only the first 256 group associations will take effect based on the association sequence. This principle also applies when the group associations are configured on an external authentication server.
Expiration	Click the button to enable **Expiration** for the user. Specify the expiration date and time. If the user expires, the user cannot be authenticated therefore is cannot be used in system. By default expiration is disabled.

Expand VPN Options, configure network parameters for the PnPVPN client.

Option	Description
IKE ID	Specifies a IKE ID type for dial-up VPN users. If FQDN or ASN1 is selected, type the ID's content in the text box below.
DHCP Start IP	Specifies a start IP for the DHCP address pool.
DHCP End IP	Specifies an end IP for the DHCP address pool.
DHCP Net-mask	Specifies a netmask for the DHCP address pool.
DHCP Gateway	Specifies a gateway for the DHCP address pool. The IP address of the gateway corresponds to the IP address of PnPVPN client's Intranet interface and PC's gateway address. The PC's IP address is determined by the segment and net-mask configured in the above DHCP address pool. Therefore, the gateway's address and DHCP address pool should be in the same segment.
DNS1	Specifies an IP address for the DNS server. You can specify one primary DNS server (DNS1) and up to three alternative DNS servers.
DNS2	
DNS3	
DNS4	
WINS1	Specifies an IP address for the WINS server. You can specify one primary WINS server (WINS1)and one alternative WINS server.
WINS2	
Tunnel IP 1	Specifies an IP address for the master PnPVPN client's tunnel interface. Select the **Enable SNAT** check box to enable SNAT.
Tunnel IP 2	Specifies an IP address for the backup PnPVPN client's tunnel interface.

3. Click **OK**.

Creating a User Group

To create a user group, take the following steps:

1. Select **Object > User > Local User** or **ZTNA > User > Local User**.
2. Click **New > User Group**.
3. Type the name of the user group into the Name box.
4. Specify members for the user group. Expand User or User Group in the Available list, select a user or user group and click **Add** to add it to the Selected list on the right. To delete a selected user or user group, select it in the Selected list and then click **Remove**. One user group can contain multiple users or user groups, but system only supports up to 12 layers of nested user groups and does not support the loopback nest. Therefore, a user group should not nest the upper-layer user group it belongs to.
5. Click **OK**.

Export User List

The system exports the user-list file in .csv format, of which the content is the real-time information of the user list in the system.

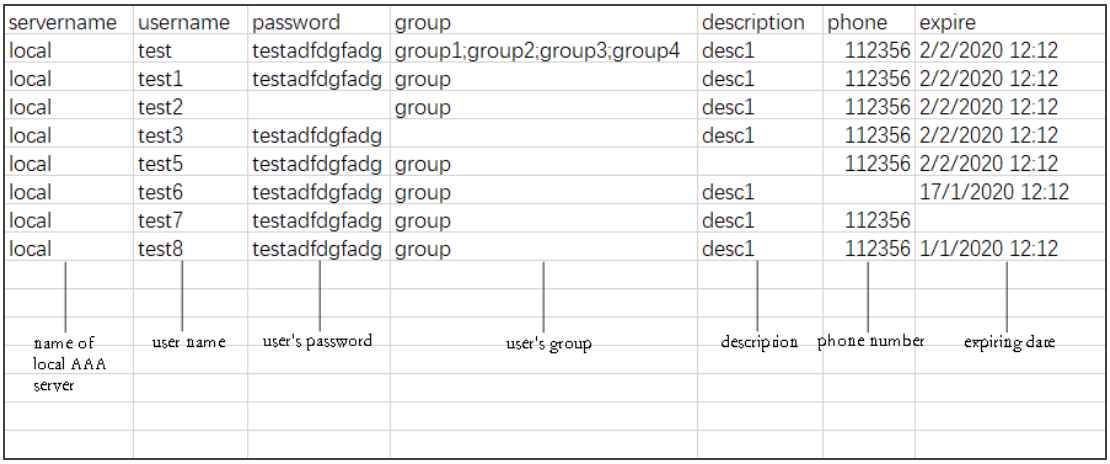
Export user binding list from system to local, take the following steps:

1. Select **Object > User > Local User** or **ZTNA > User > Local User**.
2. Click **Export User List** to open the **Export User List** page, and select the saved position in local.
3. Click **OK** to finish export.

Import User List

The system supports the import of user-list files in UTF-8 or GBK ecoding with .csv format.csv format. When the user-list file is imported, the system will carry out validity test and complexity check of the user password. If the results turn out to be successful, the importing is successful; if the results turn out to be unsuccessful, the importing is unsuccessful.

The user-list in .csv file is illustrated in the figure below.



Notes: Before importing the user-list file, please read carefully the annotations in the above figures and fill in the user information according to the format.

Import user binding list to system, take the following steps:

1. Select **Object>User> Local User** or **ZTNA > User > Local User**.
2. Click **Import User List** to open the **Import User List** page.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK** to finish import.

Notes:

- The user password in the import/export file is not encrypted, unless the password strings match the AES encryption format.
- Please try to keep the import file format consistent with the export file.
- When imported, if the same user name exists under the same server, the original user information will be overwritten.
- When imported, if a user is new to the system, it and its user information will be added to the system automatically.
- In the imported user-list file, the "username" field should not contain slash/-comma/double quotation marks/question mark/@; the "group" field should not contain comma/double quotation marks/question mark.
- In the imported user-list file, the date in the "expire" field should be typed in the format of DD/MM/YYYY HH:SS.

Configuring a LDAP User

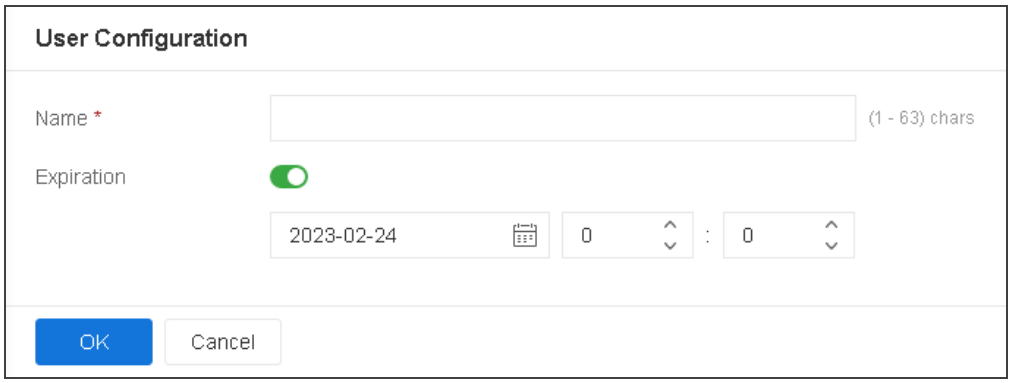
This section describes how to configure a LDAP user.

Creating a LDAP User

To create a LDAP user, take the following steps:

1. Select **Object > User > LDAP User** or **ZTNA > User > LDAP User**.

2. Click **New**.



On the User Configuration page, configure the following options.

Option	Description
Name	Enter the name of the local LDAP user.
Expiration	Turn on the switch to enable account expiration function. Select the date and time. Expired users cannot be authenticated by the device, and therefore cannot continue to use the system. By default, users do not expire.

3. Click **OK**. The newly created user will be displayed in the user list.

Notes: Locally created users can only be deleted from the firewall end.

Configuring Account Expiration

To configure account expiration for locally created users or synchronized users, take the following steps:

1. Select **Object > User > LDAP User** or **ZTNA > User > LDAP User**.
2. Select the entry you want to configure expiration, click **Edit**. Select the date and time. Expired users cannot be authenticated by the device, and therefore cannot continue to use the system. By default, users do not expire.
3. On the **User Configuration** page, turn on the switch behind **Expiration**.
4. Click **OK**.

Exporting User List

The exported user list file is in .csv format and contains the user list information currently saved by the system.

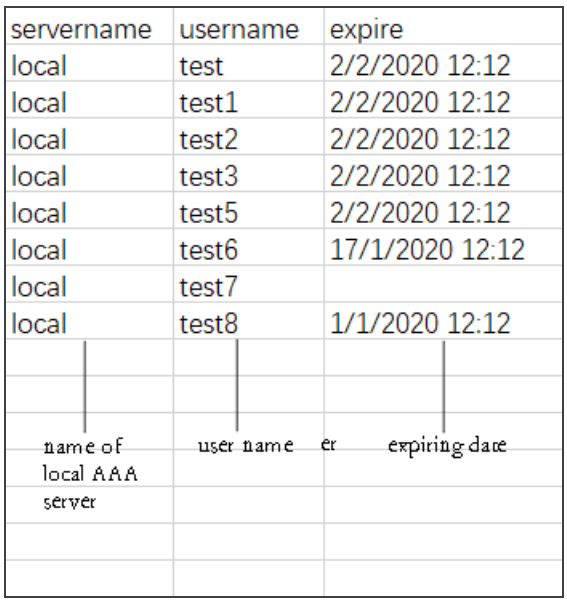
To export user list to local, take the following steps:

1. Select **Object > User > LDAP User** or **ZTNA > User > LDAP User**.
2. Click **Export User List**.
3. When the export is completed, you can see the file in your local computer.

Importing User List

The system supports importing user list files in .csv format with GBK encoding and UTF-8 encoding. During import, the system will perform validity and user password complexity checks on the entire file. If the check result is successful, the import will be completed. If the check result is unsuccessful, the import will fail.

The user-list in .csv file is illustrated in the figure below.



Notes: Before importing the user-list file, please read carefully the annotations in the above figure and fill in the user information according to the format.

To import user list to the system, take the following steps:

1. Select **Object>User> LDAP User** or **ZTNA > User > LDAP User**
2. Click **Import User List** to open the **Import User List** page.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK**.

Notes:

- Please try to keep the import file format consistent with the export file.
- When imported, if the same user name exists under the same server, the original user information will be overwritten.

- When imported, if a user is new to the system, it and its user information will be added to the system automatically.
- In the imported user-list file, the "username" field should not contain slash/-comma/double quotation marks/question mark/@; the "group" field should not contain comma/double quotation marks/question mark.
- In the imported user-list file, the date in the "expire" field should be typed in the format of DD/MM/YYYY HH:SS.

Synchronizing Users

To synchronize users in a LDAP server, firstly, you need to configure a LDAP server, refer to "Configuring LDAP Server" on Page 938. To synchronize users:

1. Select **Object > User > LDAP User** or **ZTNA > User > LDAP User**.
2. Select a server from the LDAP Server drop-down list, and click **Sync Users**.

Notes: By default, after creating a LDAP server, system will synchronize the users of the LDAP server automatically, and then continue to synchronize every 30 minutes.

Configuring an Active Directory User

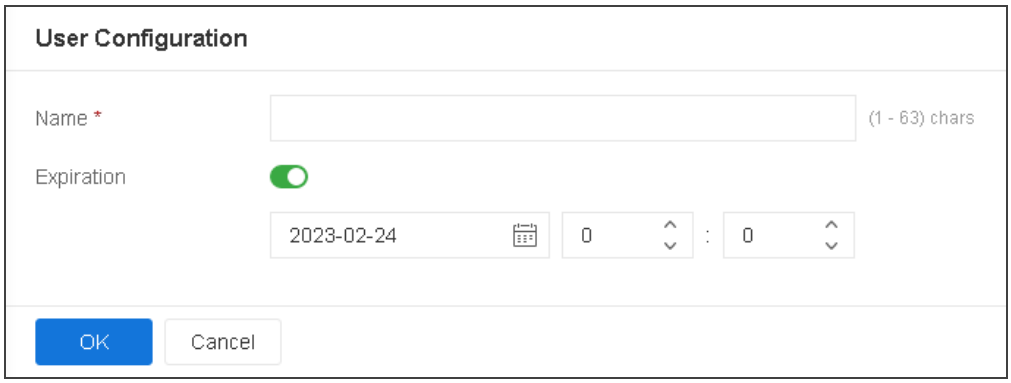
This section describes how to configure an active directory (AD) user.

Creating an Active Directory User

To create an active directory user, take the following steps:

1. Select **Object > User >AD User** or **ZTNA > User > AD User**.

2. Click **New**.



On the User Configuration page, configure the following options.

Option	Description
Name	Enter the name of the local AD user.
Expiration	Turn on the switch to enable account expiration function. Select the date and time. Expired users cannot be authenticated by the device, and therefore cannot continue to use the system. By default, users do not expire.

3. Click **OK**. The newly created user will be displayed in the user list.

Notes: Locally created users can only be deleted from the firewall end.

Configuring Account Expiration

To configure account expiration for locally created users or synchronized users, take the following steps:

1. Select **Object > User > AD User** or **ZTNA > User > AD User**.
2. Select the entry you want to configure expiration, click **Edit**. Select the date and time. Expired users cannot be authenticated by the device, and therefore cannot continue to use the system. By default, users do not expire.
3. On the **User Configuration** page, turn on the switch behind **Expiration**.
4. Click **OK**.

Exporting User List

The exported user list file is in .csv format and contains the user list information currently saved by the system.

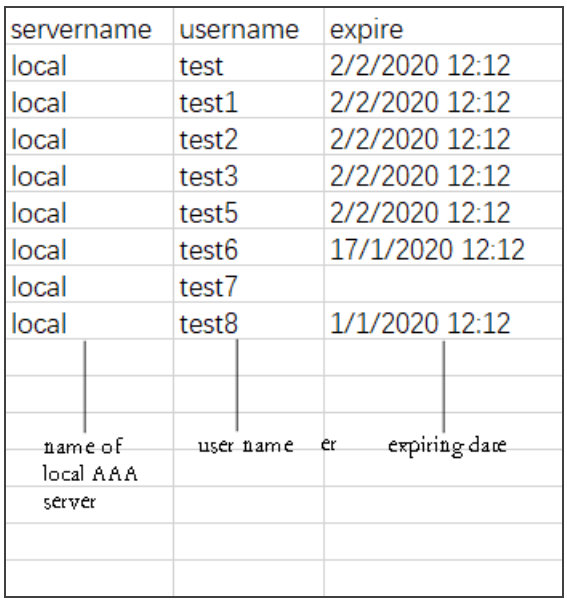
To export user list to local, take the following steps:

1. Select **Object > User > AD User** or **ZTNA > User > AD User**.
2. Click **Export User List**.
3. When the export is completed, you can see the file in your local computer.

Importing User List

The system supports importing user list files in .csv format with GBK encoding and UTF-8 encoding. During import, the system will perform validity and user password complexity checks on the entire file. If the check result is successful, the import will be completed. If the check result is unsuccessful, the import will fail.

The user-list in .csv file is illustrated in the figure below.



Notes: Before importing the user-list file, please read carefully the annotations in the above figure and fill in the user information according to the format.

To import user list to the system, take the following steps:

1. Select **Object>User> AD User** or **ZTNA > User > AD User**
2. Click **Import User List** to open the **Import User List** page.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK**.

Notes:

- Please try to keep the import file format consistent with the export file.
- When imported, if the same user name exists under the same server, the original user information will be overwritten.

- When imported, if a user is new to the system, it and its user information will be added to the system automatically.
- In the imported user-list file, the "username" field should not contain slash/-comma/double quotation marks/question mark/@; the "group" field should not contain comma/double quotation marks/question mark.
- In the imported user-list file, the date in the "expire" field should be typed in the format of DD/MM/YYYY HH:SS.

Synchronizing Users

To synchronize users in an AD server to the device, first you need to configure an AD server ,refer to "Configuring Active Directory Server" on Page 929. To synchronize users, take the following steps:

1. Select **Object > User >AD User** or **ZTNA > User > AD User**.
2. Select an AD server from the Active Directory Server drop-down list, and click **Sync Users**.

Notes: By default, after creating an AD server, system will synchronize the users of the AD server automatically, and then continue to synchronize every 30 minutes.

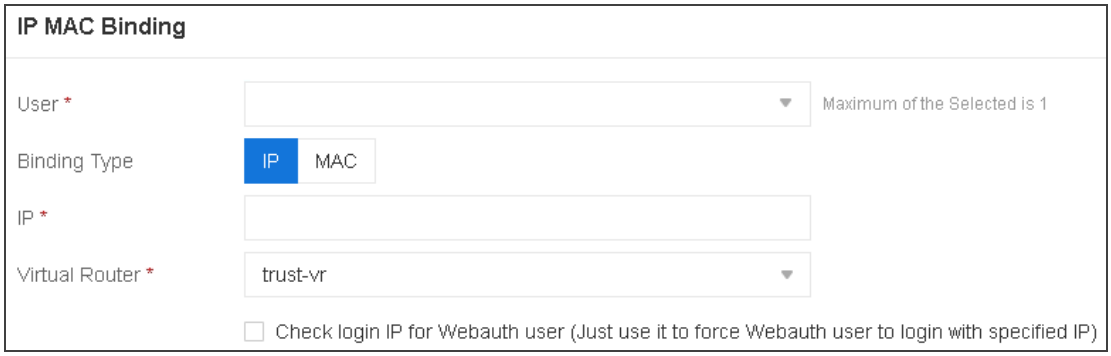
Configuring a IP-User Binding

Adding User Binding

To bind an IP or MAC address to a user, take the following steps:

1. Select **Object > User > IP-User Binding** or **ZTNA > User > IP-User Binding**.

2. Click **Add User Binding**.



Configure the following options.

User	
AAA Server	Select an AAA server from the drop-down list.
User	Select a user for the binding from the drop-down list.
Binding Type	
Binding Type	By specifying the binding type, you can bind the user to a IP address or MAC address. • IP - If IP is selected, type the IP address into the IP text box. Both the IPv4 address and IPv6 address are supported. And select a VR from the Virtual Router drop-down list. Select the **Check WebAuth IP-User Mapping Relationship** check box to apply the IP-User mapping only to the check for IP-user mapping during Web authentication if needed. • MAC - If MAC is selected, type the MAC address into

User	
	the MAC text box. And select a VR from the Virtual Router drop-down list.

3. Click **OK**.

Import Binding

Import user binding list to system, take the following steps:

1. Select **Object>User> IP-User Binding** or **ZTNA > User > IP-User Binding**..
2. Click **Import** , and the **Import User Binding List** dialog box pops up.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK** to finish import.

Export Binding

Export user binding list from system to local, take the following steps:

1. Select **Object>User> IP-User Binding** or **ZTNA > User > IP-User Binding**..
2. Select the exported user category(include local, LDAP, AD and all users) in the **Export** drop-down list to pop up the export dialog box, and select the saved position in local.
3. Click **OK** to finish export.

User Going Offline Alarm

The system supports the Going Offline Alarm function of User, which can be used to monitor the offline status of users. When the number of times that users go offline exceeds the specified threshold within a specified period of time, the system generates a corresponding event log for alarm. In addition, the system can send the alarm to related personnel by using SNMP Trap host, sms, or email in a timely manner. This facilitates subsequent response and handling.

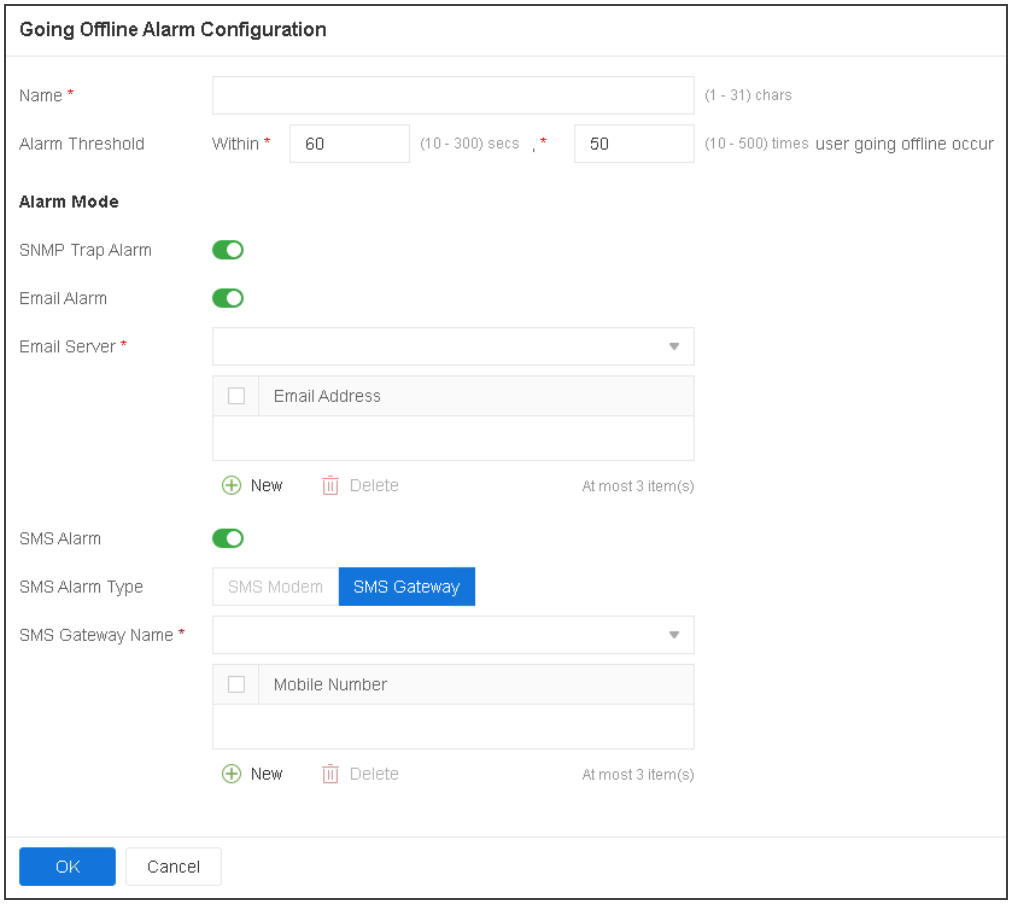
To configure the Going Offline Alarm function of User, take the following steps:

1. Creating a User Going Offline Alarm Profile.
2. Configuring an L2TP VPN Instance to Reference a User Going Offline Alarm Profile.

Creating a User Going Offline Alarm Profile

To create a user going offline alarm profile, take the following steps:

1. Select **Object** > **User** > **Going Offline Alarm**.
2. Click **New**.



On the Going Offline Alarm Configuration page, configure the following options:

Option	Description
Name	Enter the name of the user going offline alarm profile, which needs to be 1 to 31 characters in length. The name needs to be unique.
Alarm Threshold	Enter the time threshold and times threshold of user going off-line in the fields. Valid values for time: 10 to 300 seconds, default value: 60 seconds; Valid values for times: 10 to 500, default value: 50. Example, if you enter "100" and "60" respectively, an alarm will be generated when 60 times of user going offline occur within 100 seconds.
Alarm Mode	
SNMP Trap Alarm	Turn on the switch to enable the SNMP Trap Alarm function. With the function enabled, when the system generates an alarm, it will send an alarm trap message to the configured trap host. **Note:** Before you use the SNMP Trap Alarm function, you need to configure the trap host. For more information, see Trap Host.
Email Alarm	Turn on the switch to enable the Email Alarm function. With the function enabled, when the system generates an alarm, it will send an alarm notification to a specified email address. Select a configured email server from the drop-down list. 1. From the **Email Server** drop-down list, select a configured email server, or click ⊕ and create an email server in the **Mail Sever** panel. Alternatively, you can

Option	Description
	hover your mouse over a configured email server and click  to edit this email server in the **Mail Server** panel. 2. Click **New**. In the **Email Address** field, enter an email address. At most 3 email addresses can be configured. **Note:** Before you use the Email Alarm function, you need to configure the email server. For more information, see Mail Server.
SMS Alarm	Turn on the switch to enable the SMS Alarm function. With the function enabled, when the system generates an alarm, it will send an alarm notification to a specified mobile number. • When the SMS alarm type is set to SMS Modem: Click **New**. In the **Mobile Number** field, enter a mobile number. At most 3 mobile numbers can be configured. • When the SMS alarm type is set to SMS Gateway: 1. From the **SMS Gateway Name** drop-down list, select a configured SMS gateway, or click  and create an SMS gateway in the **SMS Gateway Configuration** panel. Alternatively, you can hover your mouse over a configured SMS gateway and click  to edit this SMS gateway in the **SMS Gateway Configuration** panel.

Option	Description
	2. Click **New**. In the **Mobile Number** field, enter an email address. At most 3 mobile numbers can be configured. **Note:** • Before you use the SMS Alarm function, you need to configure the SMS modem or SMS gateway. For more information, see SMS Modem and SMS Gateway. • CloudEdge supports the SMS Alarm function only by using SMS gateway.

3. Click **OK**.



Notes:

- The system can create at most 4 user going offline alarm profiles.
- Only the L2TP VPN function can reference user going offline alarm profiles. The total number of times that all user going offline alarm profiles are referenced in the system cannot exceed 8.
- When a user going offline alarm profile is referenced, you cannot modify the alarm threshold.
- At most one alarm message can be sent to a specified trap host/email address/mobile number within a minute.

Role

Roles are designed with certain privileges. For example, a specific role can gain access to some specified network resources, or make exclusive use of some bandwidth. In StoneOS, users and

privileges are not directly associated. Instead, they are associated by roles.

The mappings between roles and users are defined by role mapping rules. In function configurations, different roles are assigned with different services. Therefore, the mapped users can gain the corresponding services as well.

System supports role combination, i.e., the AND, NOT or OR operation on roles. If a role is used by different modules, the user will be mapped to the result role generated by the specified operation.

System supports the following role-based functions:

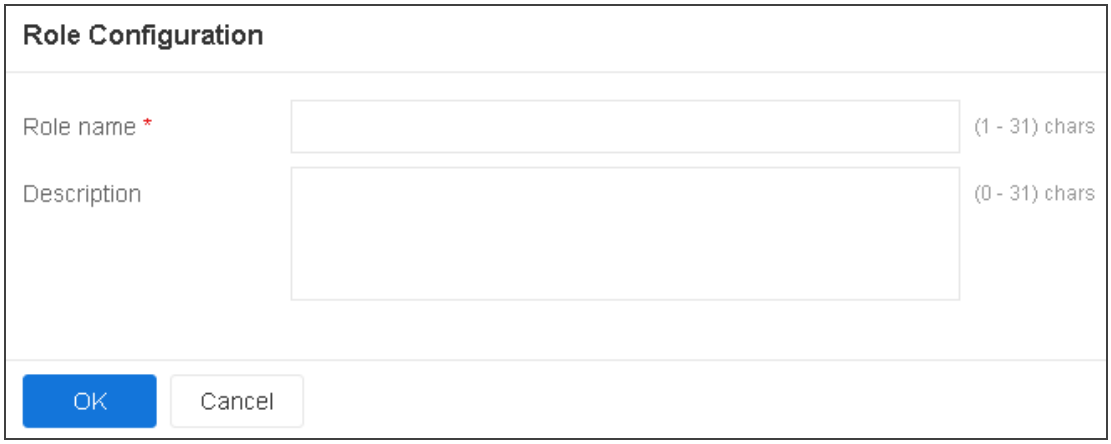
- Role-based policy rules: Implements access control for users of different types.
- Role-based QoS: Implements QoS for users of different types.
- Role-based statistics: Collects statistics on bandwidth, sessions and new sessions for users of different types.
- Role-based session limits: Implements session limits for specific users.
- SSL VPN role-based host security detection: Implements control over accesses to specific resources for users of different types.
- Role-based PBR: Implements routing for users of different types.

Configuring a Role

Creating a Role

To create a role, take the following steps:

1. Select **Object > Role > Role**.
2. Click **New**.



Option	Description
Role Name	Type the role name into the Role Name box.
Description	Type the description for the role into the Description box.

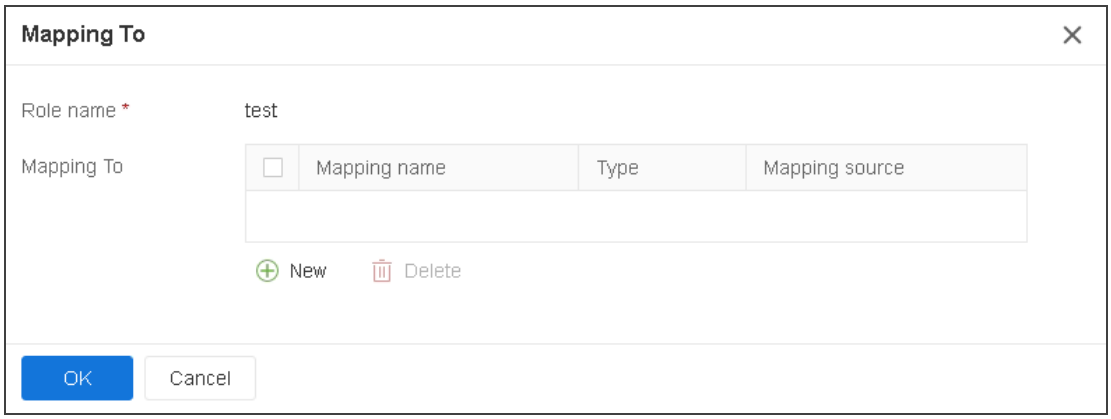
3. Click **OK**.

Mapping to a Role Mapping Rule

You can map the role to user, user group, CN, OU or the user attribute through this function or Creating a Role Mapping Rule. After Creating a Role Mapping Rule, you can click Mapping To to map the selected role again.

To map the selected role again, take the following steps:

1. Select **Object > Role > Role**.
2. Select the role need to be mapped, and click **Mapping To**.

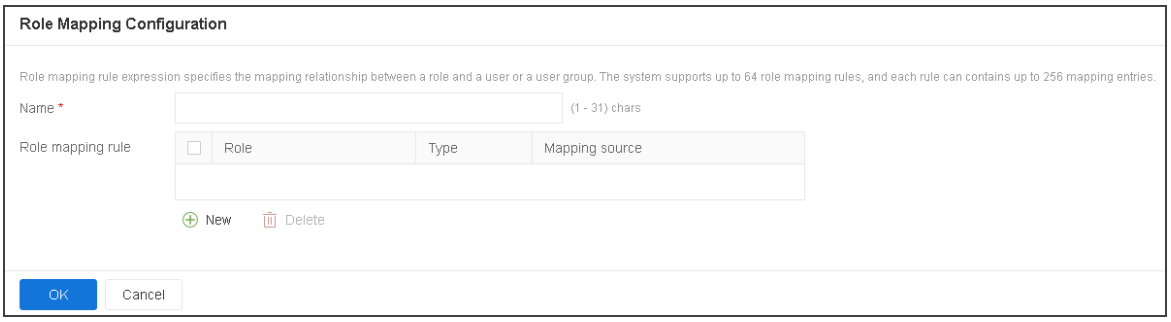


3. In the Mapping name section, select a created mapping rule name from the first drop-down list (For detailed information of creating a role mapping role, see Creating a Role Mapping Rule.), and then select a user, user group, certificate name (the CN field of USB Key certificate), organization unit (the OU field of USB Key certificate) , User Attributes, distinguished name (the DN Field of the USB Key Certificate) or any from the second drop-down list. If User, User group, CN, OU, User Attributes or DN is selected, also select or enter the corresponding user name, user group name, CN, OU, User Attributes or DN into the box behind.
4. Click **Add** to add to the role mapping list.
5. If needed, repeat Step 3 and Step 4 to add more mappings. To delete a role mapping, select the role mapping you want to delete from the mapping list, and click **Delete**.
6. Click **OK**.

Creating a Role Mapping Rule

To create a role mapping rule, take the following steps:

1. Select **Object > Role > Role Mapping** .
2. Click **New**.



3. Type the name for the rule mapping rule into the Name box.
4. In the Member section, select a role name from the first drop-down list, and then select a user, user group, certificate name (the CN field of USB Key certificate) or organization unit (the OU field of USB Key certificate) , User Attributes, , distinguished name (the DN Field of the USB Key Certificate) from the second drop-down list. If User, User group, CN, OU, User Attributes or DN is selected, also select or enter the corresponding user name, user group name, CN, OU, User Attributes or DN into the box behind.
5. Click **Add** to add to the role mapping list.
6. If needed, repeat Step 4 and Step 5 to add more mappings. To delete a role mapping, select the role mapping you want to delete from the mapping list, and click **Delete**.
7. Click **OK**.

Configuring a User Attribute Instance

To configure a user attribute instance, take the following steps:

1. Select **Object > Role > Role Mapping** .
2. Click **Configuration** in the upper-right corner, and select **User Attributes** to go to the User Attributes page.

3. Click **New** to go to the User Attributes Configuration page.



Option	Description
Name	Specifies the name of the user attribute instance.
Type	Specifies the protocol type, which can be RADIUS or AD/LDAP.
Rule Matching Policy	Specifies the rule matching policy of the user attribute instance, including: • The current rule is matched if any filter condition is met: The user is matched to the role mapped to the user attribute instance when the user hits any filter configured in the user attribute instance; • The current rule is matched if all filter conditions are met: The user is matched to the role mapped to the user attribute instance

Option	Description
	only when the user hits all filters configured in the user attribute instance.
Current Filter Conditions	Specifies the current filter conditions for this user attribute instance. Click **New** and enter the name of the user attribute in the Attributes textbox, or select a common user attribute from the dropdown list. Select the mapping operation from the **Operation** dropdown list. Enter the mapping value of the user attribute in the Value textbox.  **Notes:** • Each user attribute instance supports up to 8 filers. • When protocol type is specified as RADIUS, the mapping operation associated with string-typed user attributes can only be contain, start-with, end-with, or same-as. The mapping operation associated with number-typed user attributes can only be equal-to, greater-than, or less-than. • When the mapping operation is contain, start-with, end-with, or same-as, the mapping value can be strings or numbers. When the mapping operation is equal-to, greater-than, or less-than, the mapping value can only be numbers.

4. Click **OK** to complete the configuration. Newly created user attribute instance will be displayed on the **User Attributes** list

5. If needed, you can add more user attribute instances.

6. If you need to delete a user attribute instance, select the user attribute instance from the list, and click **Delete**.

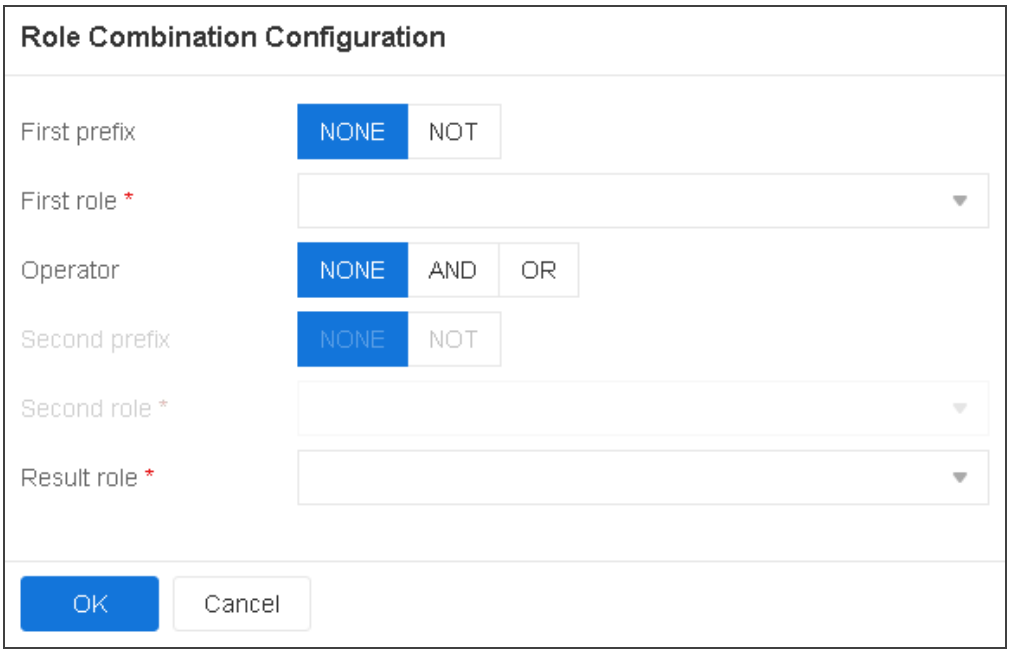
Notes: The system supports up to 64 user attributes instances.

Creating a Role Combination

To create a role combination, take the following steps:

1. Select **Object > Role > Role Combination**.

2. Click **New**.



Option	Description
First Prefix	Specifies a prefix for the first role in the role regular expression.
First Role	Select a role name from the First Role drop-down list to specify a name for the first role in the role regular expression.

Option	Description
Operator	Specifies an operator for the role regular expression.
Second Prefix	Specifies a prefix for the second role in the role regular expression.
Second Role	Select a role name from the Second Role drop-down list to specify a name for the second role in the role regular expression.
Result Role	Select a role name from the Result Role drop-down list to specify a name for the result role in the role regular expression.

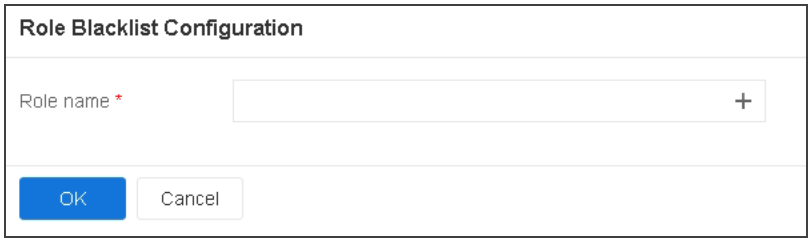
3. Click **OK**.

Creating a Role Blacklist

The system supports the role blacklist function. You can control whether a user can be successfully authenticated to log in by adding the role the user maps to in the role blacklist. During login authentication, if the role information obtained by the user via role mapping is in the role blacklist, the user cannot access the network.

To create a new role blacklist, take the following steps:

1. Select **Object > Role > Role Blacklist**.
2. On the **Role Blacklist Configuration** page, click **New**.



3. In the **Role Name** section, click + and the **Role Name** list appears. Select the role name and add it to the role blacklist. If the role information obtained by the user via role mapping is in the role blacklist, the user cannot access the network. The system supports up to 512 role

blacklists. To create a new role, click ⊕. For more information about how to create a role, refer to Creating a Role.

4. Click **OK**. You can view the newly created role blacklist entry on the role blacklist and role list.

To delete a role blacklist entry, click the check box of in front of the role blacklist entry and click Delete.

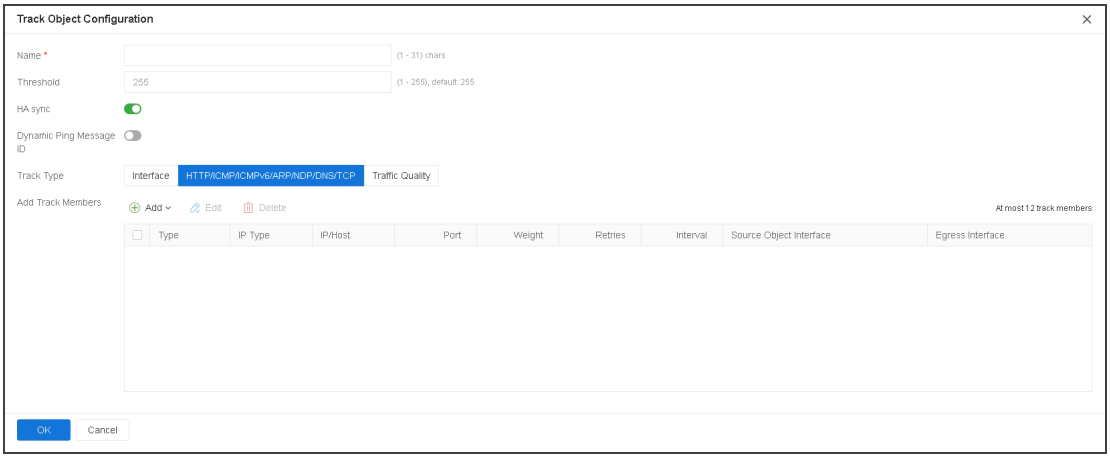
Track Object

The devices provide the track object to track if the specified object (IP address or host) is reachable or if the specified interface is connected. This function is designed to track HA and interfaces.

Creating a Track Object

To create a track object, take the following steps:

1. Select **Object > Track Object**.
2. Click **New**.



Option	Description
Name	Specifies a name for the new track object.
Threshold	Type the threshold for the track object into the text box. If the sum of weights for failed entries in the track object exceeds the threshold, system will conclude that the whole track object fails.

Track Type	Select a track object type. One track object can only be configured with one type. Select **Interface** radio button:
	• Click **Add** in Add Track Members section and then configure the following options in the Add Interfaces dialog box:
	  • Interface - Select a track interface from the drop-down list.
	  • Weight - Specifies a weight for the interface, i.e. the weight for overall failure of the whole track object if this track entry fails.
	• Edit: From the track member list, select a check box and click **Edit**. In the **Edit Interface Member** panel, edit the track member.
	• Delete: From the track member list, select a check box and click **Delete** to delete the track member.
	Select **HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP** radio button:
	• Click **Add**, select a packet type from the drop-down list,

Option	Description
	and then configure the following options in the Add HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP Member dialog box: • IP Type - Specifies the IP type for the track object when the track is implemented by HTTP/DNS/TCP packets. • IP/Host - Specifies an IP address or host name for the track object when the track is implemented by HTTP/ICMP/ICMPv6/TCP packets. IP - Specifies an IP address for the track object when the track is implemented by ARP/NDP packets. DNS - Specifies an IP address for the track object when the track is implemented by DNS packets. • Weight - Specifies a weight for overall failure of the whole track object if this track entry fails. • Retries: Specifies a retry threshold. If no response packet is received after the specified times of retries, system will determine this track entry fails, i.e., the track entry is unreachable. The value range is 1 to 255. The default value is 3. • Interval - Specifies an interval for sending packets. The value range is 1 to 255 seconds. The default

Option	Description
	value is 3. • Egress Interface - Specifies an egress interface from which HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP packets are sent. • Source Interface- Specifies a source interface for HTTP/ICMP/ICMPv6/ARP/DNS/TCP packets. • Edit: From the track member list, select a check box and click **Edit**. In the **Edit Interface Member** panel, edit the track member. • Delete: From the track member list, select a check box and click **Delete** to delete the track member.
	Select **Traffic Quality** radio button: • Click **Add** in Add Track Members section and then configure the following options in the Add Traffic Quality Member dialog box: • IP Type - Specifies the address type of the traffic quality member, including IPv4 and IPv6. When "IPv4" is specified, only the IPv4 traffic of the tracked interface; when "IPv6" is specified, only the IPv6 traffic of the tracked interface. • Interface - Specifies the name of the tracked inter-

Option	Description
	face. • Interval - Specifies the duration of per track period. The unit is second. The value range is 1 to 255. The default value is 3. After a track period is finished, system will reset the tracked value of new session. • Retries - Specifies the threshold value which concludes the track entry is failed. The value range is 1 to 255. The default value is 3. • Weight - Specifies how important this track failure is to the judgment of track object failure. The value range is 1 to 255. The default value is 255. • Low Watermark - Specifies the failure threshold value of new session success rate. The value range is 0 to 100. The default value is 30. During a track period, when the new session success rate is below the specified low watermark, system will conclude the track is failed. • High Watermark- Specifies the failure threshold value of new session success rate. The value range is 0 to 100. The default value is 50. During a track period, when the new session success rate exceeds the specified low watermark, system will conclude

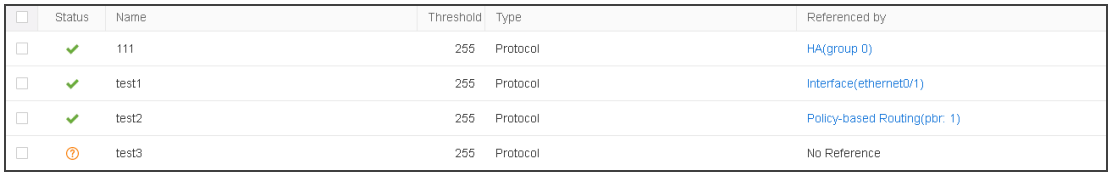
Option	Description
	the track is successful. • Edit: From the track member list, select a check box and click **Edit**. In the **Edit Interface Member** panel, edit the track member. • Delete: From the track member list, select a check box and click **Delete** to delete the track member. **Note**: During a track period, when the new session success rate is equal to or exceeds the low watermark, and is equal to or below the low watermark, system will keep the previous track state.
HA sync	Select this check box to enable HA sync function. The primary device will synchronize its information with the backup device.
Dynamic Ping Message ID	Select this check box to enable the Dynamic Ping Message ID function. With this function enabled, the header ID of ICMP messages sent by the same track object is a dynamic value. This function is disabled by default. With this function disabled, the header ID of ICMP messages sent by the same track object is a fixed value.

3. Click **OK.** The created track object will be displayed in the track object list.

Track Object List

The track object list displays information about configured track objects in the system, including **Status**, **Name**, **Threshold**, **Type**, and **Referenced by**. The **Referenced by** column displays the functional module bound to the track object, which can be an interface, HA, policy-based route, or vsys-track-status (non-root VSYS). Click the functional module to view details about the module.

When the module is unbound or unbound to the track object, the **Referenced by** column displays **No Reference**.



Status	Name	Threshold	Type	Referenced by
✔	111	255	Protocol	HA(group 0)
✔	test1	255	Protocol	Interface(ethernet0/1)
✔	test2	255	Protocol	Policy-based Routing(pbr: 1)
?	test3	255	Protocol	No Reference

Notes:

- A track object can be bound to only one module.
- In the non-root VSYS, you need to create a track object before binding it. After binding, **vsys-track-status** is displayed in the **Referenced by** column of the track object list. You cannot view details about vsys-track-status.
- In the non-root VSYS, track objects can be bound by interfaces and policy-based routes, but cannot be bound by HA. After binding, you can view details about related items in the track object list.

For information on how interfaces, HA, policy-based routes, and non-root VSYS bind track objects, see:

- Interface: An Interface binds a track object.
- HA: HA binds a track object in HA Peer Active-Active (A/A) mode/HA Active-Passive (A/P) mode.
- Policy-based Route: A policy-based route binds a track object.
- Non-root VSYS: A non-root VSYS binding a track object only support command line configuration. For details, refer to the chapter **Configuring VSYS** in the **StoneOS CLI User Guide**.

URL Filtering

URL filtering controls the access to some certain websites and records log messages for the access actions. URL filtering helps you control the network behaviors in the following aspects:

- Access control to certain category of websites, such as gambling and pornographic websites.
- Access control to certain category of websites during the specified period. For example, forbid to access IM websites during the office hours.
- Access control to the website whose URL contains the specified keywords. For example, forbid to access the URL that contains the keyword of game.

If IPv6 is enabled, you can configure URL and keyword for both IPv4 and IPv6 address. How to enable IPv6, see StoneOS_CLI_User_Guide_IPv6.

Configuring URL Filtering

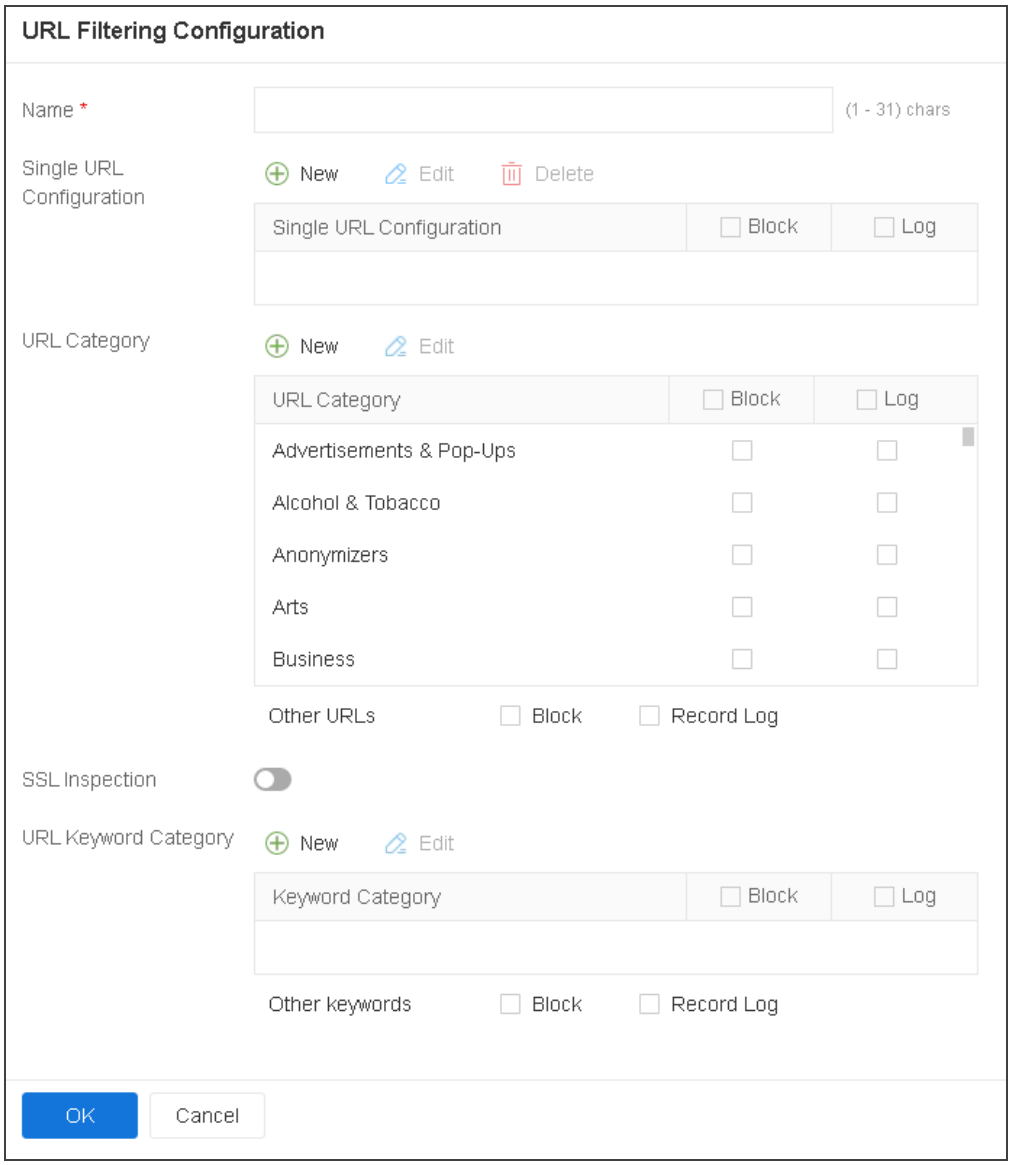
Configuring URL filtering contains two parts:

- Create a URL filtering rule
- Bind a URL filtering rule to a security zone or policy rule

Part 1: Creating a URL filtering rule

1. Select **Object > URL Filtering>Profile**.

2. Click **New**.



Configure the following options.

Option	Description
Name	Specifies the name of the rule. You can configure the same URL

Option	Description
	filtering rule name in different VSYSs.
Safe Search	Many search engines, such as Google, Bing, Yahoo!, Yandex, and YouTube, all have a "SafeSearch" setting, which can filter adult content, and then return search results at different levels based on the setting. The system supports the safe search function in the URL filtering Profile to detect the "SafeSearch" setting of search engine and perform corresponding control actions. Select the **Enable** check box to enable the safe search function to detect the settings of the search engine's "SafeSearch" and perform corresponding control actions.  Notes: • The safe search function only can be used in the following search engines currently: Google, Bing, Yahoo!, Yandex, and YouTube. • The safe search function only can be used in combination with the SSL proxy function because the search engine uses the HTTPS protocol. Therefore, when the "SafeSearch" is enabled, enable the SSL proxy function for the policy rule which is bound with URL filter profile. • To ensure the valid "SafeSearch" function

Option	Description
	 of Google, you need to configure policy rules to block the UDP 80 and UDP 443 port.
Control Action	Specifies the safe search action. o Block: Selects the check box to specify the action as block, When the " SafeSearch" setting of search engine is not set, users will be prevented from accessing the search page and a warning page will pop up which provides users with the link for "SafeSearch" setting. o Enforce: Selects the check box to specify the action as execute. When the "SafeSearch" setting of search engine is not set, system will force to set it at the “strict” level.

3. In the **URL Category** part to configure the URL category control type for URL filtering rules to control the access to some certain category of website.

In the URL Category part, configure the following options.

Option	Description
New	Creates a new URL category. For more information about URL categories, see "User-defined URL DB" on Page 1003.
Edit	Selects a URL category from the list, and click **Edit** to edit the selected URL category. **URL Keyword Category** controls the access to the website whose URL contains the specific keywords. Click the **URL Keyword Category**option to configure. The options are:

Option	Description
	• New: Creates new keyword categories. For more information about keyword category, see "Keyword Category" on Page 1007. • Edit: Select a URL keyword category from the list, and click **Edit** to edit the selected URL keyword categories. • Keyword category: Shows the name of the configured keyword categories. • Block: Selects the check box to block access to the website whose URL contains the specified keywords. • Log: Selects the check box to log the access to the website whose URL contains the specified keywords. • Other URLS: Specifies the actions to the URLs that do not contain the keywords in the list, including **Block Access** and **Record Log**.
URL category	Shows the name of pre-defined and user-defined URL categories in the VSYS.
Block	Selects the check box to block access to the corresponding URL category.
Log	Selects the check box to log access to the corresponding URL category.
Other URLs	Specifies the actions to the URLs that are not in the list, including **Block Access** and **Record Log**.

Option	Description
SSL inspection	Select the **Enable** button to enable SSL negotiation packets inspection. For HTTPS traffic, system can acquire the domain name of the site which you want to access from the SSL negotiation packets after this feature is configured. Then, system will perform URL filtering in accordance with the domain name. If SSL proxy is configured at the same time, SSL negotiation packets inspection method will be preferred for URL filtering.

4. In the **URL Keyword Category** part to configure the URL keyword category control type for URL filtering rules to control the access to the website whose URL contains the specific keywords.

In the URL Keyword Category part, configure the following options.

Option	Description
New	Creates new keyword categories. The system supports predefined keyword categories and custom keyword categories. For more information about keyword category, see "Keyword Category" on Page 1007.
Edit	Select a URL keyword category from the list, and click **Edit** to edit the selected URL keyword categories.
Keyword category	Shows the name of the configured keyword categories.
Block	Selects the check box to block access to the website whose URL contains the specified keywords.
Log	Selects the check box to log the access to the website whose

Option	Description
	URL contains the specified keywords.
Other URLs	Specifies the actions to the URLs that do not contain the keywords in the list, including **Block Access** and **Record Log**.

5. Click **OK** to save the settings.



Notes: The control type of a URL filtering rule can configure both the URL category and the URL keyword category.

Part 2: Binding a URL filtering rule to a security zone or security policy rule

The URL filtering configurations are based on security zones or policies.

- If a security zone is configured with the URL filtering function, system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the URL filtering function, system will perform detection on the traffic that is destined to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule are superior to that in a zone rule if they are specified at the same time, and the URL filtering configurations in a destination zone are superior to that in a source zone if they are specified at the same time.

To create the zone-based URL filtering, take the following steps:

1. Create a zone. For more information about how to create this, refer to "Security Zone" on Page 152.
2. In the Zone Configuration dialog box, select the Threat Protection tab.
3. Enable the threat protection that you need, and select the URL filtering rules from the profile drop-down list below; you can click **Add Profile** from the profile drop-down list below

to create a URL filtering rule. For more information, see "Part 1: Creating a URL filtering rule" on Page 992.

4. Click **OK** to save the settings.

To create the policy-based URL filtering, take the following steps:

1. Configure a security policy rule. For more information, see "Configuring a Security Policy Rule" on Page 1090.
2. In the Protection tab, select the **Enable** check box of URL Filtering.
3. From the **Profile** drop-down list, select a URL filtering rule. You can also click **Add Profile** to create a new URL filtering rule.
4. Click **OK** to save the settings.

If necessary, you can go on to configure the functions of "Predefined URL DB" on Page 1002, "URL Lookup" on Page 1005, and "Warning Page" on Page 1009.

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL categories.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database, including the URL category and the category type.
Warning Page	• Block warning: When your network access is blocked, a warning page will prompt in the Web browser. • Audit warning: When your network access is audited, a warning page will prompt in the Web browser.

Notes:

- Only after canceling the binding can you delete the URL filtering rule.
- To get the latest URL categories, you are recommended to update the URL database first. For more information about URL database, see "Predefined URL DB" on Page 1002.

Cloning a URL filtering Rule

System supports the rapid clone of a URL filtering rule. You can clone and generate a new URL filtering rule by modifying some parameters of the one current URL filtering rule.

To clone a URL filtering rule, take the following steps:

1. Select **Object > URL Filtering**.
2. Select a URL filtering rule in the list.
3. Click the **Clone** button above the list, and the **Name** configuration box will appear below the button. Then enter the name of the new URL filtering rule.
4. The cloned URL filtering rule will be generated in the list.

Viewing URL Hit Statistics

The URL access statistics includes the following parts:

- Summary: The statistical information of the top 10 user/IPs, the top 10 URLs, and the top 10 URL categories during the specified period of time are displayed.
- User/IP: The user/IP and detailed hit count are displayed.
- URL: The URL and detailed hit count are displayed.
- URL Category: The URL category and detailed hit count and traffic are displayed.

To view the URL hit statistics, see "URL Hit" on Page 1544 in Monitor.

- To view the URL hit statistics, enable **URL Hit** in "Monitor Configuration" on Page 1560.
- To view the traffic of the URL category, enable **URL Hit** and **URL Category Bandwidth** in "Monitor Configuration" on Page 1560.

Viewing Web Surfing Records

To view the Web surfing records, view "URL Log" on Page 1581. Before you view the Web surfing records, see "Log Configuration" on Page 1602 to enable URL Log function.

Configuring URL Filtering Objects

When using URL filtering function, you need to configure the following objects:

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL categories.
User-defined URL DB	The user-defined URL database is defined by you and you can use it to specify the URL category.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Keyword Category	Use the keyword category function to view the predefined keyword categories and customize the keyword categories. For more information about keyword category, see Keyword Category in URL Filtering.
Warning Page	Enable or disable the warning page. • Block warning: When your network access is blocked, a warning page will prompt in the Web browser.

Object	Description
	• Audit warning: When your network access is audited, a warning page will prompt in the Web browser.

Predefined URL DB

System contains a predefined URL database.



Notes: The predefined URL database is controlled by a license . Only after a URL license is installed, the predefined URL database can be used.

The predefined URL database provides URL categories for the configurations of a URL filtering. It includes dozens of categories and tens of millions of URLs .

When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

Configuring Predefined URL Database Update Parameters

By default, system updates predefined URL database everyday. You can change the update parameters according to your own requirements. Currently, two default update servers are provided: https://update1.hillstonenet.com and https://update2.hillstonenet.com. Besides, you can update the predefined URL database from your local disk. For more information about how to change the update parameters, see Updating Signature Database.

Upgrading Predefined URL Database Online

To upgrade the URL database online, take the following steps:

1. Select **System > Upgrade Management > Signature Database Update**.
2. In the URL category database update section, click **Update** to update the predefined URL database.

Upgrading Predefined URL Database from Local

To upgrade the predefined URL database from local, take the following steps:

1. **System > Upgrade Management > Signature Database Update**
2. In the URL category database update section, click **Browse** to select the URL database file from your local disk.
3. Click **Upload** to update the predefined URL database.



Notes: You can not upgrade the predefined URL database from local in non-root VSYS.

User-defined URL DB

Besides categories in predefined URL database, you can also create user-defined URL categories, which provides URL categories for the configurations of URL filtering. When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

System provides three predefined URL categories: custom1, custom2, custom3. You can import your own URL lists into one of the predefined URL categories.



Notes: You can not import your own URL lists into one of the predefined URL category in non-root VSYS.

Configuring User-defined URL DB

To configure a user-defined URL category, take the following steps:

1. Select **Object > URL Filtering**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.

3. Click **New**. The URL Category dialog box will appear.



4. Type the category name in the **Category** box. URL category name cannot only be a hyphen (-). And you can create at most 16 user-defined categories.
5. Type a URL into the **URL http(s)://** box.
6. Click **Add** to add the URL and its category to the table.
7. To edit an existing one, select it and then click **Edit**. After editing it, click **Add** to save the changes.
8. Click **OK** to save the settings.

Importing User-defined URL

System supports to batch imported user-defined URL lists into the predefined URL category named custom1/2/3. To import user-defined URL, take the following steps:

1. Select **Object > URL Filtering**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.
3. Select one of the predefined URL category(custom1/2/3), and then click **Import**.

4. In the Batch Import URL dialog box, click **Browse** button to select your local URL file. The file should be less than 1 M, and have at most 1000 URLs. Wildcard is supported to use once in the URL file, which should be located at the start of the address.

5. Click **OK** to finish importing.

Clearing User-defined URL

In the predefined URL category named custom1/2/3, clear a user-defined URL, take the following steps:

1. Select **Object > URL Filtering**.

2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog box will appear.

3. Select one of the predefined URL categories(custom1/2/3), and then click **Clear**. The URL in the custom 1/2/3 will be cleared from the system.

URL Lookup

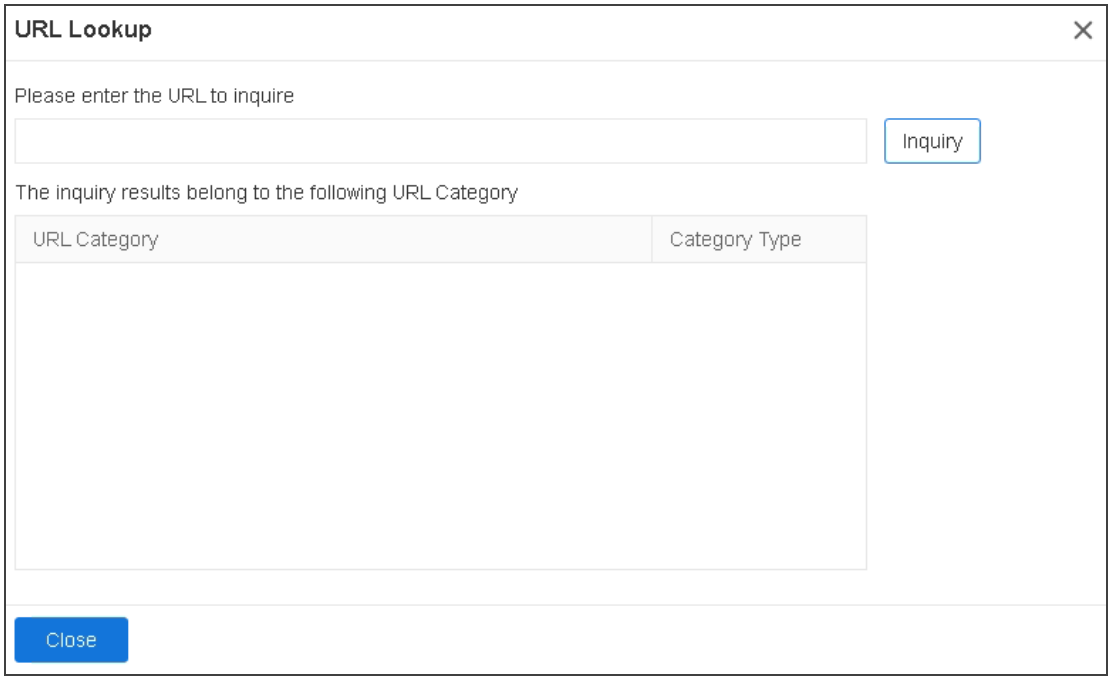
You can inquire a URL to view the details by URL lookup, including the URL category and the category type.

Inquiring URL Information

To inquiry URL information, take the following steps:

1. Select **Object > URL Filtering**.

2. At the top-right corner, click **Configuration > URL Lookup**. The URL Lookup dialog box will appear.



3. Type the URL into the **Please enter the URL to inquire** box.

4. Click **Inquire**, and the results will be displayed at the bottom of the dialog box.

Configuring URL Lookup Servers

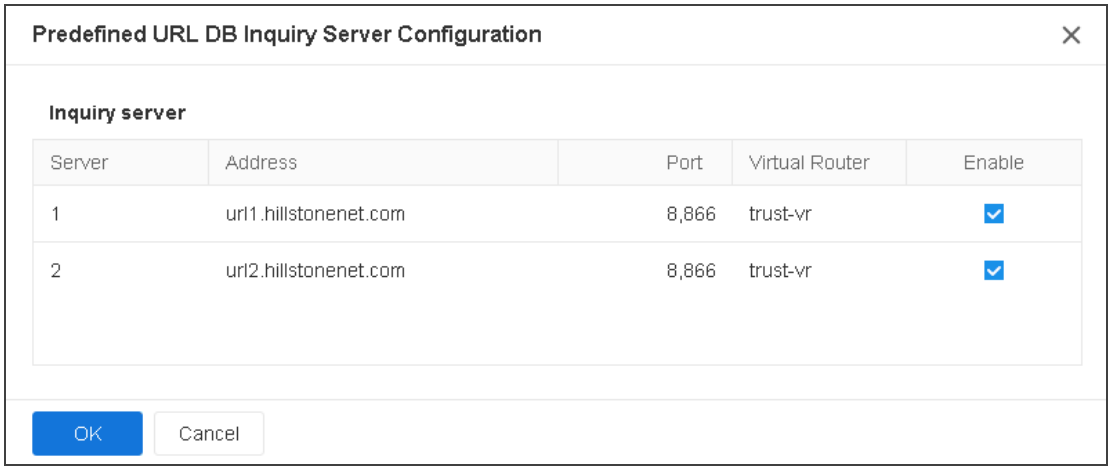
URL lookup server can classify an uncategorized URL (URL is neither in predefined URL database nor in user-defined URL database) you have accessed, and then add it to the URL database during database updating. Two default URL lookup servers are provided: url1.hillstonenet.com and url2.hillstonenet.com. By default, the URL lookup servers are enabled.

To configure a URL lookup server, take the following steps:

1. Select **Object > URL Filtering>Profile**.

2. At the top-right corner, Select **Configuration > Predefined URL DB**. The Predefined URL DB dialog box will appear.

3. Click **Inquiry Server Configuration**. The Predefined URL DB Inquiry Server Configuration dialog box will appear.



4. In the Inquiry server section, double-click the cell in the IP/Port/Virtual Router column of Server1/2 and type a new value.
5. Select the check box in the **Enable** column to enable this URL lookup server.
6. Click **OK** to save the settings.

Keyword Category

Keyword categories include predefined keyword categories and custom keyword categories, which are used in the URL filtering function. You can use predefined keyword categories or customize the keyword category as needed. System provide four predefined keyword categories, which are **predef_bank_card** (keyword for bank card number), **predef_email_address** (keyword for email address), **predef_cellphone_number** (keyword for mobile phone number), and **predef_mainland_id_card** (keyword for ID number), which cannot be edited or deleted.

After configuring a URL filtering rule, system will scan traffic according to the configured keywords and calculate the trust value for the hit keywords. The calculating method is: adding up the results of *times * trust value* of each keyword that belongs to the category. Then system compares the sum with the threshold 100 and performs the following actions according to the comparison result:

- If the sum is larger than or equal to category threshold (100), the configured category action will be triggered;
- If more than one category action can be triggered and there is block action configured, the final action will be Block;
- If more than one category action can be triggered and all the configured actions are Permit, the final action will be Permit.

For example, a URL filtering rule contains two keyword categories C1 with action block and C2 with action permit. Both of C1 and C2 contain the same keywords K1 and K2. Trust values of K1 and K2 in C1 are 20 and 40. Trust values of K1 and K2 in C2 are 30 and 80.

If system detects 1 occurrence of K1 and K2 each on a URL, then C1 trust value is 20*1＋40*1-1=60<100, and C2 trust value is 30*1+80*1=110>100. As a result, the C2 action is triggered and the URL access is permitted.

If system detects 3 occurrences of K1 and 1 occurrence of K2 on a URL, then C1 trust value is 20*3+40*1=100, and C2 trust value C2 is 30*3+80*1=170>100. Conditions for both C1 and C2 are satisfied, but the block action for C1 is triggered, so the web page access is denied.

Configuring a Keyword Category

To configure a keyword category, take the following steps:

1. Select **Object > URL Filtering**.
2. At the top-right corner, select **Configuration > Keyword Category**. The Keyword Category page will appear.
3. Display predefined keyword categories and created custom keyword categories in the Keyword Category page.

4. Click **New**. The **Keyword Category Configuration** page will appear.



5. Type the category name.
6. Click **New** and specify the keyword, character matching method (simple/regular expression), and trust value (100 by default).
7. Repeat the above steps to add more keywords.
8. To delete a keyword, select the keyword you want to delete from the list and click **Delete**.
9. Click **OK** to save your settings.

Warning Page

The warning page shows the user block information and user audit information. You can enable or disable the warning page as needed.

The warning page include predefined warning page and user-defined warning page.

- Predefined warning page: Displays the predefined warning information content, including prompt information and warning reasons.
- User-defined warning page: You can customize the warning page by custom warning information and pictures. For details, please refer to "Warning Page Management" on Page 1745..

Enabling/ Disabling the Block Warning

The block warning is disabled by default. If the internet behavior is blocked by the URL filtering function, the Internet access will be denied. The information of Access Denied will be shown in your browser, and some web surfing rules will be shown to you on the warning page at the same time. According to the different network behaviors, the predefined warning page includes the following two situations:

- Visiting a certain type of URL.

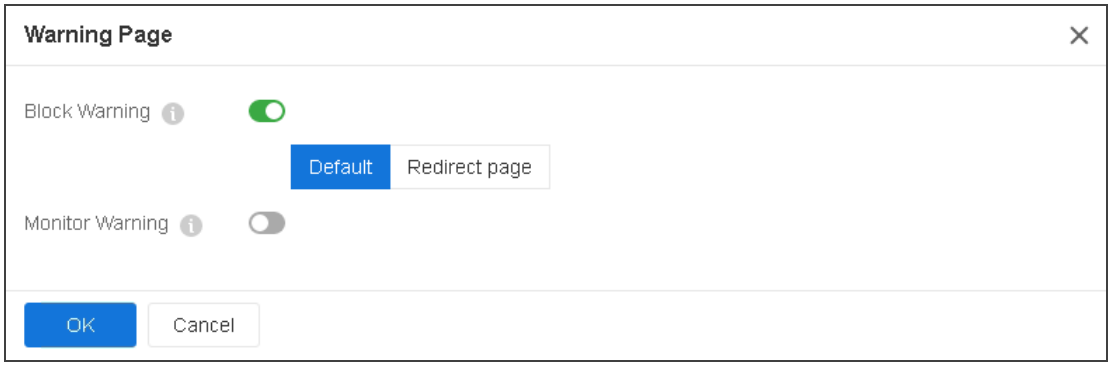


- Visiting the URL that contains a certain type of keyword category.



To enable or disable the block warning , take the following steps:

1. Click **Object > URL Filtering > Profile**.
2. At the top-right corner, select **Configuration > Warning Page**. The Warning Page dialog box will appear.



3. In the Block Warning section, select **Enable**. To disable this function, unselect the **Enable** check box.

4. Configure the display information in the blocking warning page.

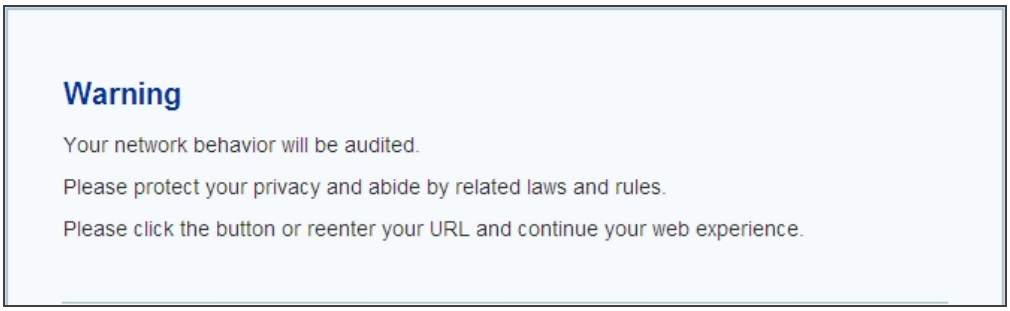
Option	Description
Default	Use the default blocking warning page as shown above. After selecting the **Default** radio button: • If the user-defined warning page is not configured, the pre-defined warning page will be used. • If the user-defined warning page is configured and enabled, the user-defined warning page will be used.
Redirect page	Redirect to the specified URL. Type the URL in the **URL http://** box. You can click Detection to verify whether the URL is valid.

5. Click **OK** to save the settings.

Enabling/ Disabling the Audit Warning

The audit warning function is disabled by default. After enabling the audit warning function, when your network behavior matches the configured URL filtering rule, your HTTP request will be

redirected to a warning page where the audit and privacy protection information is displayed. See the picture below:



To enable or disable the audit warning function, take the following steps:

1. Select **Object > URL Filtering**.
2. At the top-right corner, select **Configuration > Warning Page**. The Warning Page dialog box will appear.
3. In the Audit Warning section, select **Enable**.To disable this function, unselect the **Enable** check box.
   - If the user-defined warning page is not configured, the predefined warning page will be used.
   - If the user-defined warning page is configured and enabled, the user-defined warning page will be used.

   For details, please refer to "Warning Page Management" on Page 1745..
4. Click **OK** to save the settings.

First Access of Uncategorized URL

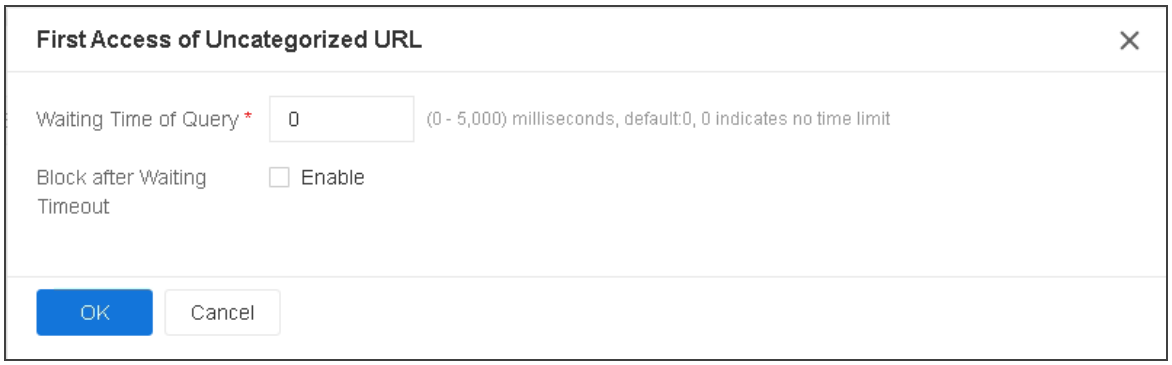
For the uncategorized URL that you visit for the first time, that is, the URL which is neither in the system's predefined URL database nor in the user-defined URL database, system will continue to query the category of the URL in the cloud. Because the query may takes a litter while, system cannot process the uncategorized URL immediately until the query result is returned.

To solve the above problem, you can specify the waiting time of query and enable the block action when waiting times out. After the waiting time of query is exceeded, system will block the access to the uncategorized URL.

To configure related content of the first access of an uncategorized URL, take the following steps:

Select **Object** > **URL Filtering** > **Profile**.

At the top-right corner, select **Configuration** > **First Access of Uncategorized URL**. The First Access of Uncategorized URL dialog box will appear.



Type the waiting time value of query into the Waiting Time of Query text box. The range is 0 to 5000ms. The default value is 0, which means there is no wait time limit.

Select the Enable check box after Block after Waiting Timeout to enable the block action, after the waiting time of query is exceeded, system will block the access of uncategorized URL. After clearing the Enable check box, after the waiting time of query is exceeded, system will continue to perform URL filtering according to the configuration of URL filtering profile.

Click **OK** to save the settings.

Configuring the URL Blacklist/Whitelist

You can further control the access to some websites by configuring URL blacklists and whitelists.

- After the URL blacklist is configured, when you send an access request to the specified URL in the blacklist, the system will block the request.

- After the URL whitelist is configured, when you send an access request to the specified URL in the whitelist, system will not perform URL filtering for the access request and let the request pass
- The URL blacklist, the URL whitelist and the URL filtering rule all configured with URL categories, the matching priority for URL category filtering is: the URL blacklist > the URL whitelist > the URL filtering rule.



Notes:

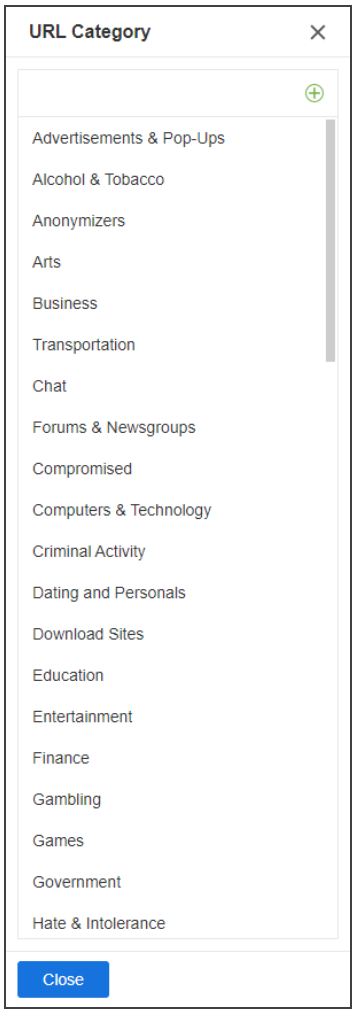
- An URL category can only be referenced by an object (URL blacklist, URL whitelist or URL filtering profile). For example, when the URL category "Advertisement" has been added to the URL blacklist, this URL category cannot be added to the URL whitelist, and it will not be referenced in the URL filtering profile.
- Non-root VSYS does not support the URL blacklist\whitelist function, and the URL blacklist/whitelist configuration under root VSYS does not take effect and has no effect on non-root VSYS.

Configuring the URL Blacklist

To configure the URL blacklist, take the following steps:

1. Select **Object > URL Filtering > URL Blacklist/Whitelist**.
2. Select **URL Blacklist** tab to open the URL blacklist page, which displays all URL categories that have been added to the URL blacklist and the corresponding URL type and description.

3. Click "+" , and select the add the URL category needed to add to the URL black list.



4. The "URL category" on the left contains all URL categories that can be referenced (pre-defined URL DB and user-defined URL DB). You can also click ⊕ to create a new URL category. For specific steps, see Configuring User-defined URL DB.

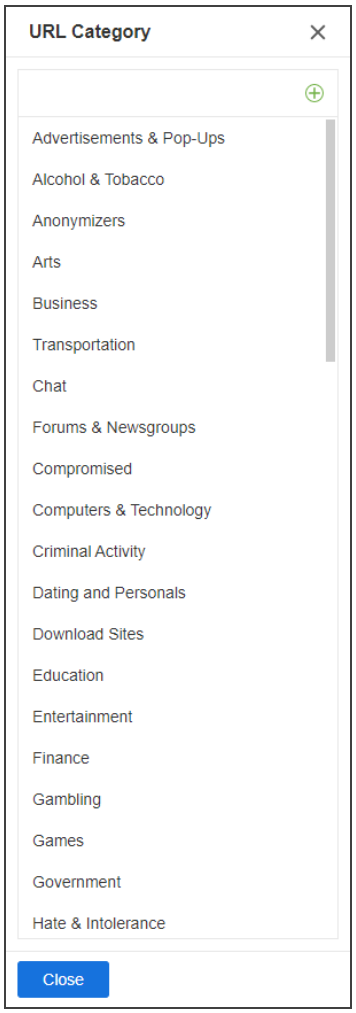
5. If you need to delete the URL category entry in the URL blacklist, in the "URL blacklist" list on the right, select the URL category entry you want to delete and click ✕ .

6. Click **OK**.

Configuring the URL Whitelist

To configure the URL whitelist, take the following steps:

1. Select **Object > URL Filtering > URL Blacklist/Whitelist**.
2. Select **URL Whitelist** tab to open the URL whitelist page, which displays all URL categories that have been added to the URL whitelist and the corresponding URL type and description.
3. Click "+" , and select the add the URL category needed to add to the URL white list.



4. The "URL category" on the left contains all URL categories that can be referenced (pre-defined URL DB and user-defined URL DB). You can also click ⊕ to create a new URL category. For specific steps, see Configuring User-defined URL DB.
5. If you need to delete the URL category entry in the URL whitelist, in the "URL whitelist" list on the right, select the URL category entry you want to delete and click ✕ .
6. Click **OK**.

Data Security

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

The data security function allows you to flexibly configure control rules to comprehensively control and audit (by behavior logs and content logs) on user network behavior.

Data security can audit and filter in the following network behaviors:

Function	Description
File filter	Checks the files transported through HTTP(S), FTP, SMTP(S), IMAP (S), POP3(S), SMB protocols and control them according to the file filter rules.

Content filter	• File content filter: Detect sensitive keywords carried in the file content of the specified protocol type and file type, and can log or block them.
	• Web content :Controls the network behavior of visiting the webpages that contain certain keywords, and log the actions.
	• Web posting: Controls the network behavior of posting on websites and posting specific keywords, and logs the posting action and posted content.
	• Email filter: Controls and audit SMTP(S)/POP3(S)/IMAP (S)mails :
	  • Control and audit all the behaviors of sending emails;
	  • Control and audit the behaviors of sending emails that contain specific sender, recipient, keyword or attachment.
	• Application behavior control: Controls and audits the actions of

Function	Description
	HTTP(S), FTP and TELNET applications: • FTP contents and methods, including Login, Get, and Put; • HTTP(S) methods, including Connect, Get, Put, Head, Options, Post, and Trace; • Request content initiated by the TELNET client.
Network Behavior Record	Audits the IM applications behaviors and record log messages for the access actions.

Configuring Objects

Objects mean the items referenced during Content Filter rules. When using the data security function, you need to configure the following objects:

Object	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL DB	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Keyword Category	Use the keyword category function to view the predefined keyword categories and customize the keyword categories. You can use it to specify the keyword for the File Content Filter/Web Content/Web

Object	Description
	Posting/Email filter/HTTP(S)/FTP Control functions. For more information about keyword category, see Keyword Category in Data Security.
Warning Page	Enable or disable the warning page. • Block warning: When your network access is blocked, a warning page will prompt in the Web browser. • Audit warning: When your network access is audited, a warning page will prompt in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
Exempt User	Users that are not controlled by the internet behavior control rules.

Predefined URL DB

The system contains a predefined URL database.

Notes: The predefined URL database is controlled by a license controlled. Only after a URL license is installed, the predefined URL database can be used.

The predefined URL database provides URL categories for the configurations of Web content/Web posting. It includes dozens of categories and tens of millions of URLs .

When identifying the URL category of a URL, the user-defined URL database has a higher priority than the predefined URL database.

Configuring Predefined URL Database Update Parameters

By default, the system updates predefined URL database everyday. You can change the update parameters according to your own requirements. Currently, two default update servers are provides: https://update1.hillstonenet.com and https://update2.hillstonenet.com. Besides, you

can update the predefined URL database from your local disk. For more information about how to change the update parameters, see Updating Signature Database.

Upgrading Predefined URL Database Online

To upgrade the URL database online:

1. Select **System > Upgrade Management > Signature Database Update**.
2. In the URL category database update section, click **Update** to update the predefined URL database.

Upgrading Predefined URL Database from Local

To upgrade the predefined URL database from local:

1. **System > Upgrade Management > Signature Database Update**
2. In the URL category database update section, click **Browse** to select the URL database file from your local disk.
3. Click **Upload** to update the predefined URL database.

User-defined URL DB

Besides categories in predefined URL database, you can also create user-defined URL categories, which provides URL categories for the configurations of Web content/Web posting. When identifying the URL category, the user-defined URL database has a higher priority than the predefined URL database.

System provides three predefined URL categories: custom1, custom2, custom3. You can import your own URL lists into one of the predefined URL category.

Configuring User-defined URL DB

To configure a user-defined URL category:

1. Select **Object > URL Filtering> Profile**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.
3. Click **New**. The URL Category dialog appears.



4. Type the category name in the **Category** box. URL category name cannot only be a hyphen (-). And you can create at most 16 user-defined categories.
5. Type a URL into the **URL http(s)://** box.
6. Click **Add** to add the URL and its category to the table.
7. To edit an existing one, select it and then click **Edit**. After editing it, click **Add** to save the changes.
8. Click **OK** to save the settings.

Importing User-defined URL

System supports to batch import user-defined URL lists into the predefined URL category named custom1/2/3. To import user-defined URL:

1. Select **Object > URL Filter**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.
3. Select one of the predefined URL category(custom1/2/3), and then click **Import**.
4. In the Batch Import URL dialog, click **Browse** button to select your local URL file. The file should be less than 1 M, and has at most 1000 URLs. Wildcard is supported to use once in the URL file, which should be located at the start of the address.
5. Click **OK** to finish importing.

Clearing User-defined URL

In the predefined URL category named custom1/2/3, clear user-defined URL:

1. Select **Object > URL Filter**.
2. At the top-right corner, select **Configuration > User-defined URL DB**. The User-defined URL DB dialog appears.
3. Select one of the predefined URL category(custom1/2/3), and then click **Clear**, the URL in the custom 1/2/3 will be cleared from the system.

URL Lookup

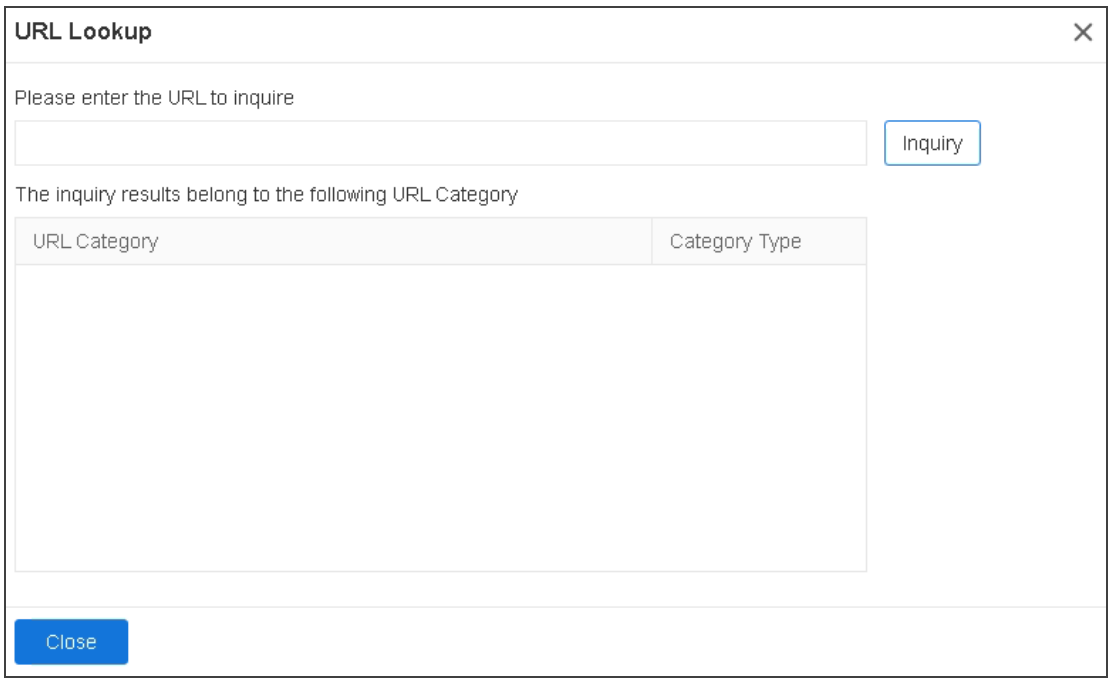
You can inquire a URL to view the details by URL lookup, including the URL category and the category type.

Inquiring URL Information

To inquiry URL information:

1. Select **Object > URL Filtering> Profile**.

2. At the top-right corner, click **Configuration > URL Lookup**. The URL Lookup dialog appears.



3. Type the URL into the **Please enter the URL to inquire** box.

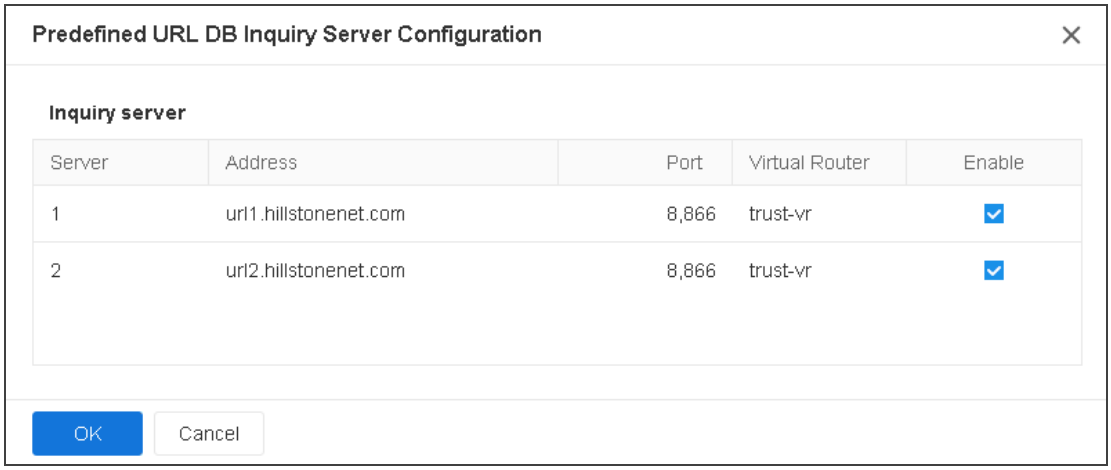
4. Click **Inquire**, and the results will be displayed at the bottom of the dialog.

Configuring URL Lookup Servers

URL lookup server can classify an uncategorized URL (URL is neither in predefined URL database nor in user-defined URL database) you have accessed, and then add it to the URL database during database updating. Two default URL lookup servers are provided: url1.hillstonenet.com and url2.hillstonenet.com. By default, the URL lookup servers are enabled.

To configure a URL lookup server:

1. Select **Object > URL Filtering> Profile**.
2. At the top-right corner, Select **Configuration > Predefined URL DB**. The Predefined URL DB dialog appears.
3. Click **Inquiry Server Configuration**. The Predefined URL DB Inquiry Server Configuration dialog appears.



4. In the Inquiry server section, double-click the cell in the IP/Port/Virtual Router column of Server1/2 and type a new value.
5. Select the check box in the **Enable** column to enable this URL lookup server.
6. Click **OK** to save the settings.

Keyword Category

Keyword categories include predefined keyword categories and custom keyword categories, which are used in the URL filtering function. You can use predefined keyword categories or customize the keyword category as needed. System provide four predefined keyword categories, which are **predef_bank_card** (keyword for bank card number), **predef_email_address** (keyword for email address), **predef_cellphone_number** (keyword for mobile phone number), and **predef_mainland_id_card** (keyword for ID number), which cannot be edited or deleted.

After configuring a internet behavior control rule, the system will scan traffic according to the configured keywords and calculate the trust value for the hit keywords. The calculating method is: adding up the results of *times * trust value* of each keyword that belongs to the category. Then the system compares the sum with the threshold 100 and performs the following actions according to the comparison result:

- If the sum is larger than or equal to category threshold (100), the configured category action will be triggered;
- If more than one category action can be triggered and there is block action configured, the final action will be Block;
- If more than one category action can be triggered and all the configured actions are Permit, the final action will be Permit.

For example, a web content rule contains two keyword categories C1 with action block and C2 with action permit. Both of C1 and C2 contain the same keywords K1 and K2. Trust values of K1 and K2 in C1 are 20 and 40. Trust values of K1 and K2 in C2 are 30 and 80.

If the system detects 1 occurrence of K1 and K2 each on a web page, then C1 trust value is 20*1＋40*1=60<100, and C2 trust value is 30*1+80*1=110>100. As a result, the C2 action is triggered and the web page access is permitted.

If the system detects 3 occurrences of K1 and 1 occurrence of K2 on a web page, then C1 trust value is 20*3+40*1=100, and C2 trust value C2 is 30*3+80*1=170>100. Conditions for both C1 and C2 are satisfied, but the block action for C1 is triggered, so the web page access is denied.

Configuring a Keyword Category

To configure a keyword category:

1. Select **Object > URL Filtering> Profile**.
2. At the top-right corner, Select **Configuration > Keyword Category**. The Keyword Category page appears.

3. Display predefined keyword categories and created custom keyword categories in the Keyword Category page.
4. Click **New**. The **Keyword Category Configuration** page appears.



5. Type the category name.
6. Click **New** and specify the keyword, character matching method (simple/regular expression), and trust value (100 by default).
7. Repeat the above steps to add more keywords.
8. To delete a keyword, select the keyword you want to delete from the list and click **Delete**.
9. Click **OK** to save your settings.

Warning Page

The warning page shows the user block information and user audit information. You can enable or disable the warning page as needed.

The warning page includes predefined warning page and user-defined warning page.

- Predefined warning page: Displays the predefined warning information content, including prompt information and warning reasons.

- User-defined warning page: You can customize the warning page by custom warning information and pictures. For details, please refer to "Warning Page Management" on Page 1745..

Enabling/ Disabling the Block Warning

The block warning is disabled by default. If the internet behavior is blocked by the internet behavior control function, the Internet access will be denied. The information of Access Denied will be shown in your browser, and some web surfing rules will be shown to you on the warning page at the same time. The predefined warning page below:



After enabling the block warning function, block warning information will be shown in the browser when one of the following actions is blocked:

- Visiting the web page that contains a certain type of keyword category
- Posting information to a certain type of website or posting a certain type of keywords
- HTTP actions of Connect, Get, Put, Head, Options, Post, and Trace.

To enable or disable the block warning:

1. Click **Object > URL Filtering> Profile**.

2. At the top-right corner, Select **Configuration > Warning Page**. The Warning Page dialog appears.



3. In the Block Warning section, select **Enable**.To disable this function, unselect the **Enable** check box.

   - If the user-defined warning page is not configured, the predefined warning page will be used.
   - If the user-defined warning page is configured and enabled, the user-defined warning page will be used.

   For details, please refer to "Warning Page Management" on Page 1745..

4. Click **OK** to save the settings.

Enabling/ Disabling the Audit Warning

The audit warning function is disabled by default. After enabling the audit warning function, when your internet behavior matches the configured internet behavior rules, your HTTP request will be redirected to a warning page, on which the audit and privacy protection information is displayed. See the picture below:



To enable or disable the audit warning function:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.
2. At the top-right corner, Select **Configuration > Warning Page**. The Warning Page dialog appears.
3. In the Audit Warning section, select **Enable**.To disable this function, unselect the **Enable** check box.
   - If the user-defined warning page is not configured, the predefined warning page will be used.
   - If the user-defined warning page is configured and enabled, the user-defined warning page will be used.

   For details, please refer to "Warning Page Management" on Page 1745..
4. Click **OK** to save the settings.

Bypass Domain

Regardless of internet behavior control rules, requests to the specified bypass domains will be allowed unconditionally.

To configure a bypass domain:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.

2. At the top-right corner, Select **Configuration > Bypass Domain**. The Bypass Domain dialog appears.



3. Click **New**.In the text box, type the domain name. The domain name will be added to the system and displayed in the bypass domain list.

4. Click **OK** to save the settings.

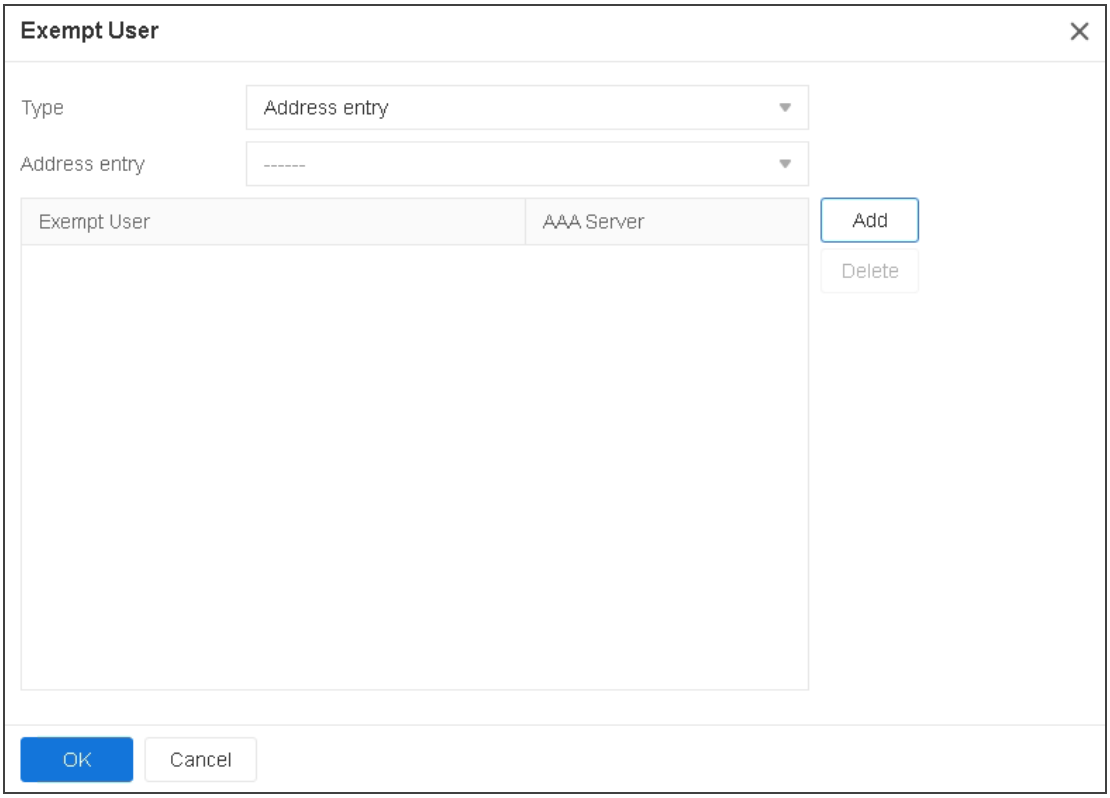
Exempt User

The Exempt User function is used to specify the users who will not be controlled by the internet behavior control rules. The system supports the following types of exempt user: IP, IP range, role, user, user group, and address entry.

To configure the user exception:

1. Select **Object > Data Security>Content Filter> Web Content/Web Posting/Email Filter/HTTP/FTP Control**.

2. At the top-right corner, Select **Configuration > Exempt User**. The Exempt User dialog appears.



3. Select the type of the user from the **Type** drop-down list.
4. Configure the corresponding options.
5. Click **Add**. The user will be added to the system and displayed in the exempt user list.
6. Click **OK** to save the settings.

File Filter

The file filter function checks the files transported through HTTP(S), FTP, SMTP(S), IMAP(S), POP3(S), SMB protocols and control them according to the file filter rules.

- Be able to check and control the files transported through GET and POST methods of HTTP (S), FTP, SMTP(S), IMAP(S), SMB, and POP3(S). If SMB protocol type is used, the system supports the detection and controlling of files in break-point resumption scenarios.
- Support file type filter conditions.
- Support block, log, and permit actions.

After you bind the file filter profile to a policy rule, the system will process the traffic that matches the rule according to the profile. The system also supports binding the file filter profile to a ZTNA policy to perform file detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

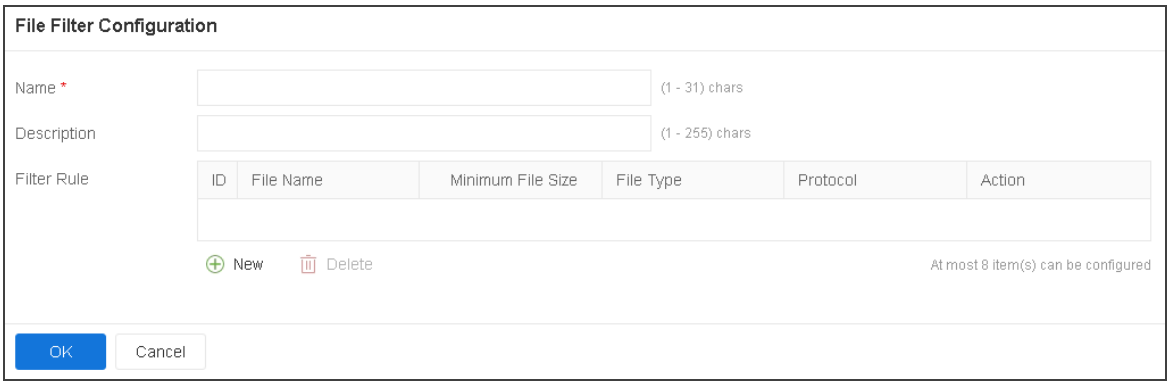
Creating File Filter Rule

Use the file filter rule to specify the protocol that you want to check, the filter conditions, and the actions.

To create a file filter rule:

1. Select **Object > Data Security > File Filter**.

2. Click **New**.



3. In the dialog box, enter values.

Option	Description
Name	Specifies the name of the file filter rule.
Description	Specifies the description of the file filter rule.
Filter Rule	
ID	The ID of file filter rule item. There can be up to 8 items in each file filtering rule. Click the + button to add a file filter rule item. If one filter rule item is configured with the block action and the file happens to match this rule, then the system will block the uploading/downloading of this file.
Minimum File Size	When the size of the transported file reaches the specified file size, the system will trigger the actions. The range is from 1 to 512,000. The unit is KB.
File Type	Specify the file type. Click on the column's cells and select from the drop-down menu. You can specify more than one file types. To control the file type that not supported, you can use the

Option	Description
	UNKNOWN type. When the transmitted file is a particular type, the system will trigger the actions. The file filter function can identify the following file types: 7Z, AI, APK, ASF, AVI, BAT, BMP, CAB, CATPART, CDR, CIN, CLASS, CMD, CPL, DLL, DOC, DOCX, DPX, DSN, DWF, DWG, DXF, EDIT, EMF, EPS, EPUB, EXE, EXR, FLA, FLV, GDS, GIF, GZ, HLP, HTA, HTML, IFF, ISO, JAR, JPG, KEY, LNK, LZH, MA, MB, MDB, MDI, MIF, MKV, MOV, MP3, MP4, MPEG, MPKG, MSI, NUMBERS, OCX, PAGES, PBM, PCL, PDF, PGP, PIF, PL, PNG, PPT, PPTX, PSD, RAR, REG, RLA, RMVB, RPF, RTF, SGI, SH, SHK, STP, SVG, SWF, TAR, TDB, TIF, TORRENT, TXT, VBE, WAV, WEBM, WMA, WMF, WMV, WRI, WSF, XLS, XLSX, XML, XPM, ZIP, BZ2, UNKNOWN
Protocol	Specifies the protocols. http-get represents to check the files transported through the GET method of HTTP. http-post represents to check the files transported through the POST method of HTTP. ftp represents to check the files transported through FTP. smtp represents to check the files transported through SMTP. imap represents to check the files transported through IMAP. pop3 represents to check the files transported through POP3. You can specify more than one protocol types. This option is required.
Action	Specify the action to control the files that matches the filter con-

Option	Description
	ditions. You can specify block or log. This option is required.

4. Click **OK**.

Viewing File Filter Logs

To view the file filter logs, refer to "File Filter Log" on Page 1582.

Content Filter

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Includes:

- "File Content Filter" on Page 1037: Detect and control the behavior of sensitive keywords carried in the file content of the specified transmission protocol type and file type.
- "Web Content" on Page 1042: Controls the network behavior of visiting the webpages that contain certain keywords, and log the actions.
- "Web Posting" on Page 1048: Controls the network behavior of posting on websites and posting specific keywords, and logs the posting action and posted content.
- "Email Filter" on Page 1054: Controls and audit SMTP(S)/POP3(S)/IMAP(S) mails :
  - Control and audit all the behaviors of sending emails.
  - Control and audit the behaviors of sending emails that contain specific sender, recipient, keyword or attachment.
- "APP Behavior Control" on Page 1059:Controls and audits the actions of HTTP(S) and FTP applications:

- FTP methods, including Login, Get, and Put.
- HTTP(S) methods, including Connect, Get, Put, Head, Options, Post, Delete and Trace.
- Request content initiated by the TELNET client.

File Content Filter

The file content filtering function can detect sensitive keywords carried in the file content of the specified protocol type and file type, and can log or block them. For example, the content of doc-type files downloaded through the HTTP protocol is detected, and the log information is recorded for the files containing the keyword content of the mobile phone number.

Configuring File Content Filter

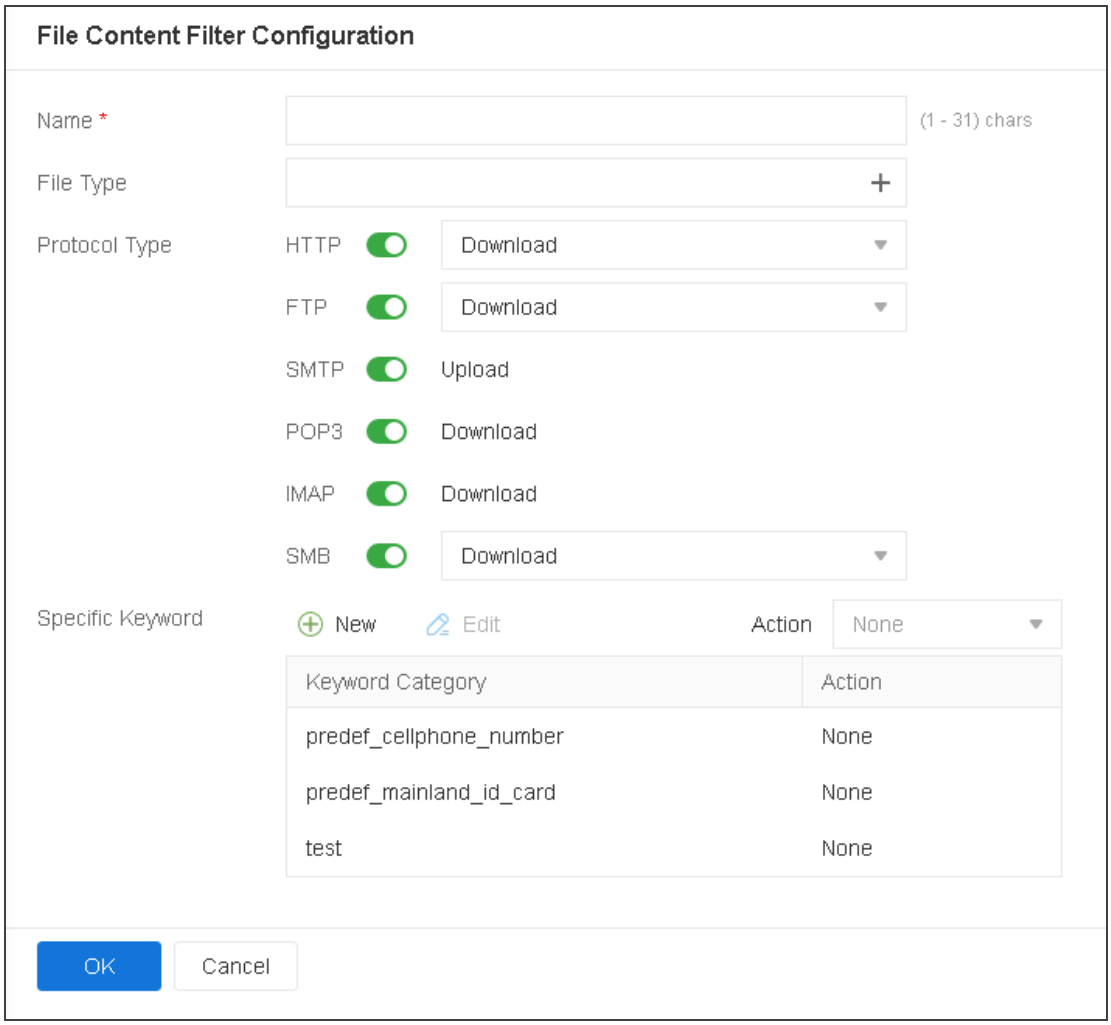
Configuring file content filter contains two parts:

- Create a file content filter rule
- Bind a file content filter rule to a security zone or policy rule. The system also supports binding the file content filter profile to a ZTNA policy to perform file content detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

Part 1: Creating a file content filter rule

1. Select **Object > Data Security > Content Filter > File Content Filter**

2. Click **New**.



Option	Description
Name	Specifies the rule name.
File Type	Specifies the file type. Click the + button and select the file type in the **File Type** page, you can specify one or more file types. Currently supported file types are: txt, doc, docx, ppt, pptx, xls, xlsx.

Option	Description
Protocol Type	Specifies the detected file transfer protocol and direction. Click the **Enable** button after the specified protocol type, and select the detection direction from the drop-down list. HTTP, FTP, and SMB protocols support Download, Upload, and Bidirectional; SMTP protocol only supports select Upload; POP3 and IMAP protocols only support Download.
Specific Keyword	Specifies the keyword category for filtering and the action. 1. All predefined keyword categories and custom keyword categories displayed in this partial list. 2. Select the control action in the **Action** drop-down list, including None, Log Only, and Block (block and record log). 3. Click the **New** to configure the keywords that need to be controlled in the **Keyword Category Configuration** page. For more information about keyword category, see "Configuring Objects" on Page 1019.

3. Click **OK**.

Part 2: Binding a file content filter rule to a security zone or security policy rule

The file content filter configurations are based on security zones or policies.

- If a security zone is configured with the file content filter function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.

- If a policy rule is configured with the file content filter function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the file content filter configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based file content filter:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 152.
2. In the Zone Configuration dialog, click **Data Security** .
3. Enable the File Content Filter, and select a file content filter rule from the profile drop-down list below; or you can click ⊕ from the profile drop-down list below, to create a file content filter rule, see Configuring File Content Filter.
4. Click **OK** to save the settings.

To realize the policy-based file content filter:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 1090.
2. Click **Data Security** to expand the option, click the **Enable** button of File Content Filter.
3. From the **Profile** drop-down list, select a file content filter rule. You can also click ⊕ to create a new file content filter rule.
4. Click **OK** to save the settings.

Viewing Monitored Results of Keyword Blocking in File Content

If you have configured file content filter with keyword blocking, you can view the monitored results of blocking those words.

Select **Monitor > Keyword Block > File Content**, you will see the monitored results. For more about monitoring, refer to File Content.

Viewing Logs of Keyword Blocking in File Content

To see the system logs of keyword blocking in file content, please refer to the "Content Filter Log" on Page 1583.

Web Content

The web content function is designed to control the network behavior of visiting the websites that contain certain keywords. For example, you can configure to block the access to website that contains the keyword "gamble", and record the access action and website information in the log.

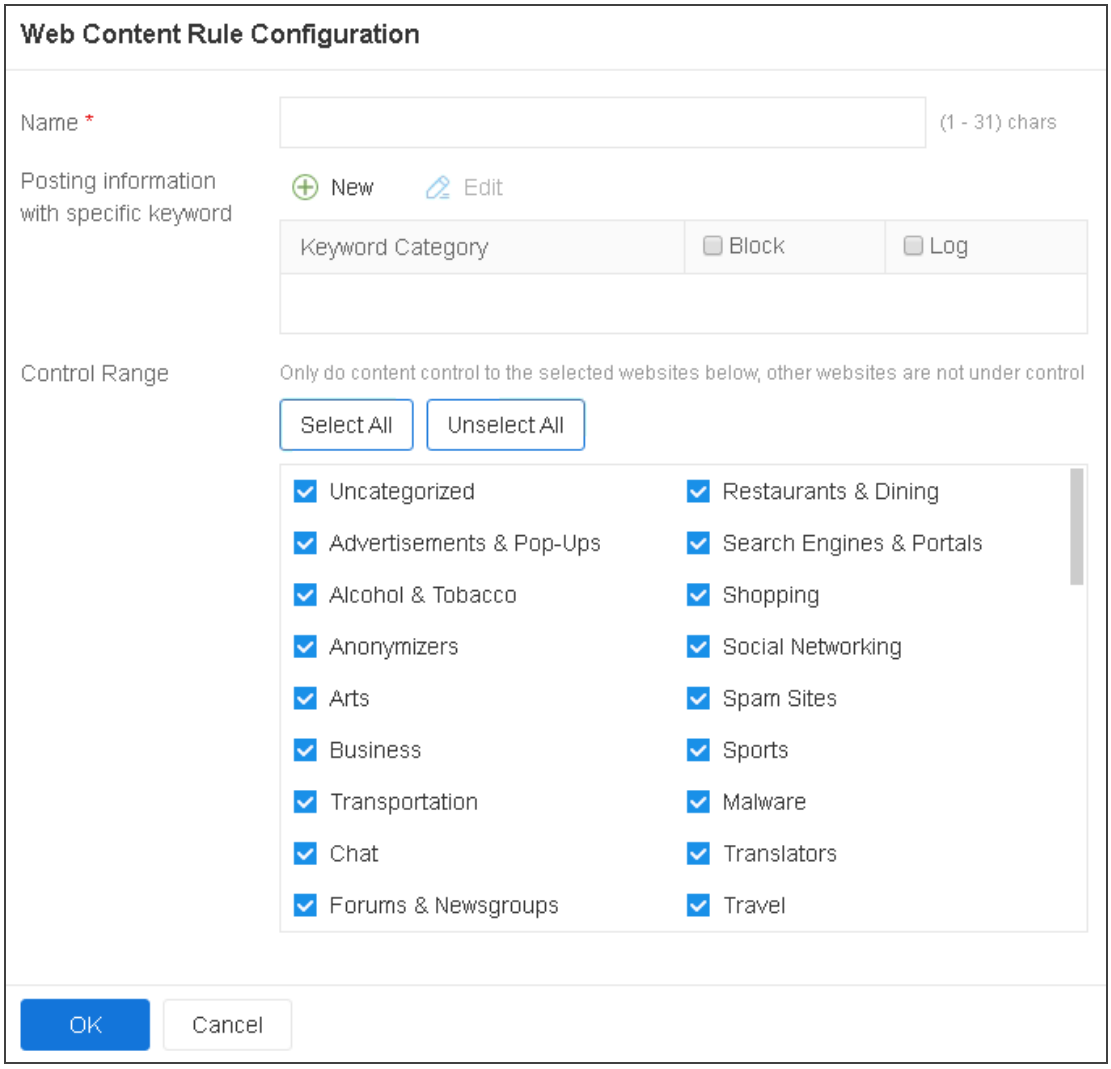
Configuring Web Content

Configuring Web Content contains two parts:

- Create a Web Content rule
- Bind a Web Content rule to a security zone or policy rule

Part 1: Creating a web content rule

1. Select **Object > Data Security > Content Filter > Web Content**.
2. Click **New**.



Option	Description
Name	Specifies the rule name.
Posting information with specific keyword	Defines the action when a keyword is matched. • New: Creates new keyword categories. For more information about keyword category, see "Configuring Objects" on Page 1019. • Edit: Edits selected keyword category.

Option	Description
	• Keyword category: Shows the name of configured keyword categories. • Block: Select the check box to block the web pages containing the corresponding keywords. • Log: Select the check box to record log messages when visiting the web pages containing the corresponding keywords. • Record contents: Select the check box to record the keyword context. This option is available only when the device has a storage media (SD card, U disk, or storage module provided by Hillstone) with the NBC license installed.
Control Range	Specify the coverage of this rule. By default, the rule applies to all website. 1. Click **Control Range**. 2. Select or unselect the websites you want to monitor and control. 3. Click **OK**.

3. Click **OK**.

Part 2: Binding a Web Content rule to a security zone or security policy rule

The Web content configurations are based on security zones or policies.

- If a security zone is configured with the Web content function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the Web content function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the Web content configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based Web Content:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 152.
2. In the Zone Configuration dialog, click Data Security to expand the option.
3. Enable the Web content, and select a Web content rules from the profile drop-down list below; or you can click ⊕ from the profile drop-down list below, to create a Web content rule, see Creating a Web content rule.
4. Click **OK** to save the settings.

To realize the policy-based Web content:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 1090.
2. Click **Data Security** to expand the option, click the **Enable** button ofWeb Content.
3. From the **Profile** drop-down list, select a Web Content rule. You can also click ⊕to create a new Web Content rule.
4. Click **OK** to save the settings.

If necessary, you can configure some additional features by going to the right top corner and click **Configuration**.

Option	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL DB	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Warning Page	• Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser. • Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
User Exception	Users that are not controlled by the internet behavior control rules.



Notes:

- To enusre you have the latest URL database, it is better to update your database first. Refer to "Configuring Objects" on Page 1019.
- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1602.

- By default, a rule will immediately take effect after you click **OK** to complete configuration.

Viewing Monitored Results of Keyword Blocking in Web Content

If you have configured email filter with keyword blocking, you can view the monitored results of blocking those words.

Select **Monitor > Keyword Block > Web Content**, you will see the monitored results. For more about monitoring, refer to "Web Content" on Page 1539.

Viewing Logs of Keyword Blocking in Web Content

To see the system logs of keyword blocking in web content, please refer to the "Content Filter Log" on Page 1583.

Web Posting

The web posting function can control the network behavior of posting on websites and posting specific keywords, and can log the posting action and posting content. For example, forbid the users to post information containing the keyword X, and record the action log.

Configuring Web Posting

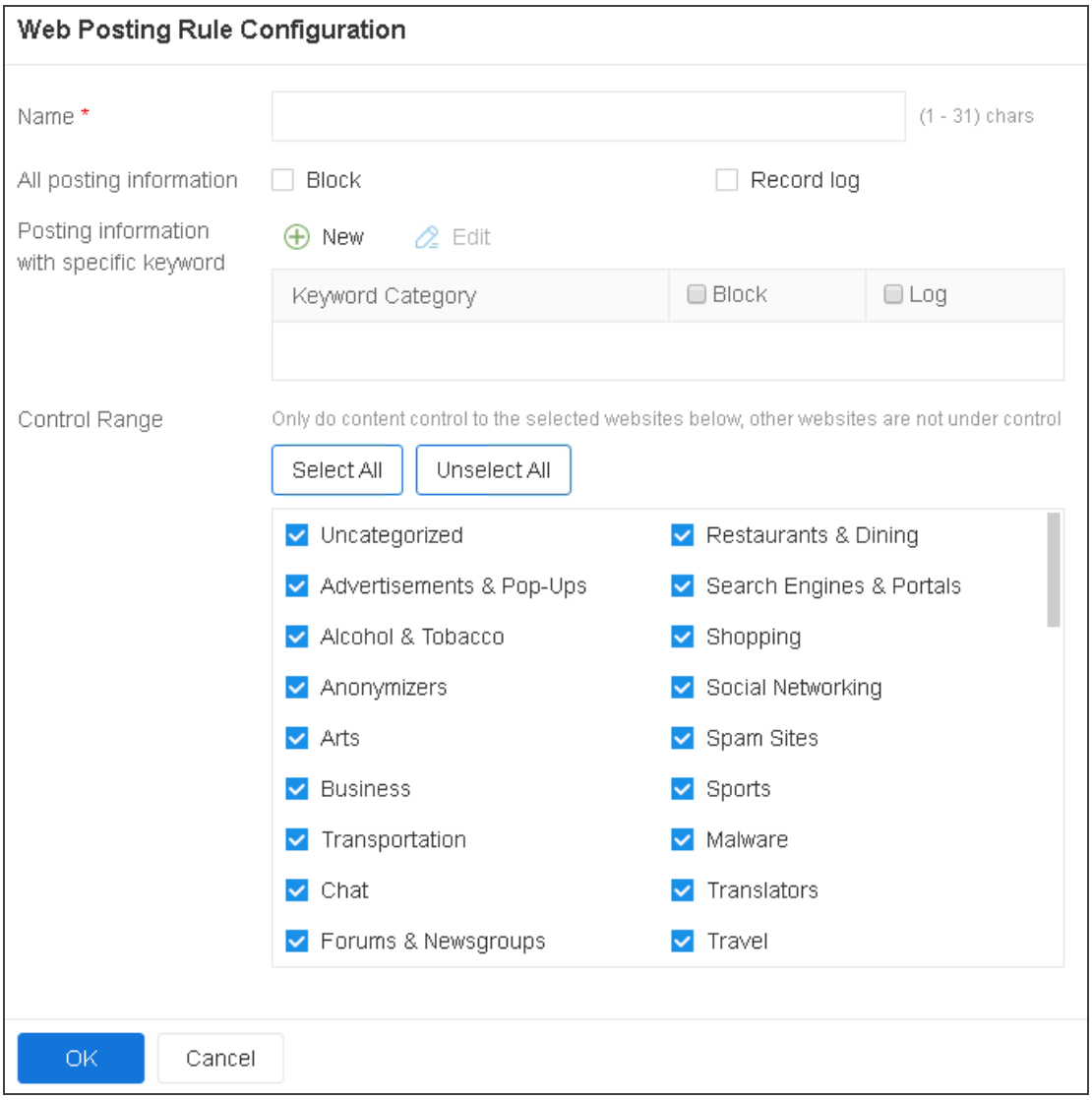
Configuring Web Posting contains two parts:

- Create a web posting rule
- Bind a web posting rule to a security zone or policy rule

Part 1: Creating a web posting rule

1. Select **Object > Data Security > Content Filter > Web Posting**.

2. Click **New**.



Option	Description
Name	Specifies the rule name.
All posting information	The action applies to all web posting content. • Block: Select to block all web posting behaviors.

Option	Description
	• Record Log: Select to record all logs about web posting.
Posting information with specific keyword	Controls the action of posting specific keywords. The options are: • New: Creates new keyword categories. For more information about keyword category, see "Keyword Category" on Page 1025. • Edit: Edits selected keyword category. • Keyword category: Shows the name of configured keyword categories. • Block: Blocks the posting action of the corresponding keywords. • Log: Records log messages when posting the corresponding keywords.
Control Range	Specify the coverage of this rule. By default, the rule applies to all website. 1. Click **Control Range**. 2. Select or unselect the websites you want to monitor and control. 3. Click **OK**.

3. Click **OK**.

Part 2: Binding a Web Posting rule to a security zone or security policy rule

The web posting configurations are based on security zones or policies.

- If a security zone is configured with the web posting function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the web posting function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the web posting configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based web posting:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 152.
2. In the Zone Configuration dialog, select Data Security tab.
3. Enable the threat protection you need, and select a Web content rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create a Web content rule, see Creating a web posting rule.
4. Click **OK** to save the settings.

To realize the policy-based web posting:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 1090.
2. In the Data Security tab, select the **Enable** check box of web posting.
3. From the **Profile** drop-down list, select a web posting rule. You can also click **Add Profile** to create a new web posting rule.
4. Click **OK** to save the settings.

If necessary, you can configure some additional features by going to the right top corner and click **Configuration**.

Option	Description
Predefined URL DB	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL DB	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
URL Lookup	Use the URL lookup function to inquire URL information from the URL database.
Warning Page	• Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser. • Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
User Exception	Users that are not controlled by the internet behavior control rules.



Notes:

- To enusre you have the latest URL database, it is better to update your database first. Refer to "Configuring Objects" on Page 1019.
- If there is an action conflict between setting for "all websites" and "specific keywords", when a traffic matches both rules, the "deny" action shall prevail.

- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1602.
- By default, a rule will immediately take effect after you click **OK** to complete configuration.

Viewing Monitored Results of Keyword Blocking in Web Posts

If you have configured web posting rule with keyword blocking, you can view the monitored results of blocking those words.

Select **Monitor > Keyword Block > Web Posting**, you will see the monitored results. For more about monitoring, refer to "Keyword Block" on Page 1538.

Viewing Logs of Keyword Blocking in Web Posts

To see the system logs of keyword blocking in web posts, please refer to the "Content Filter Log" on Page 1583.

Email Filter

The email filter function is designed to control the email sending actions according to the sender, receiver, email content and attachment, and record the sending log messages. Both the SMTP (S)/POP(S)/IMAP(S) emails and the web mails can be controlled.

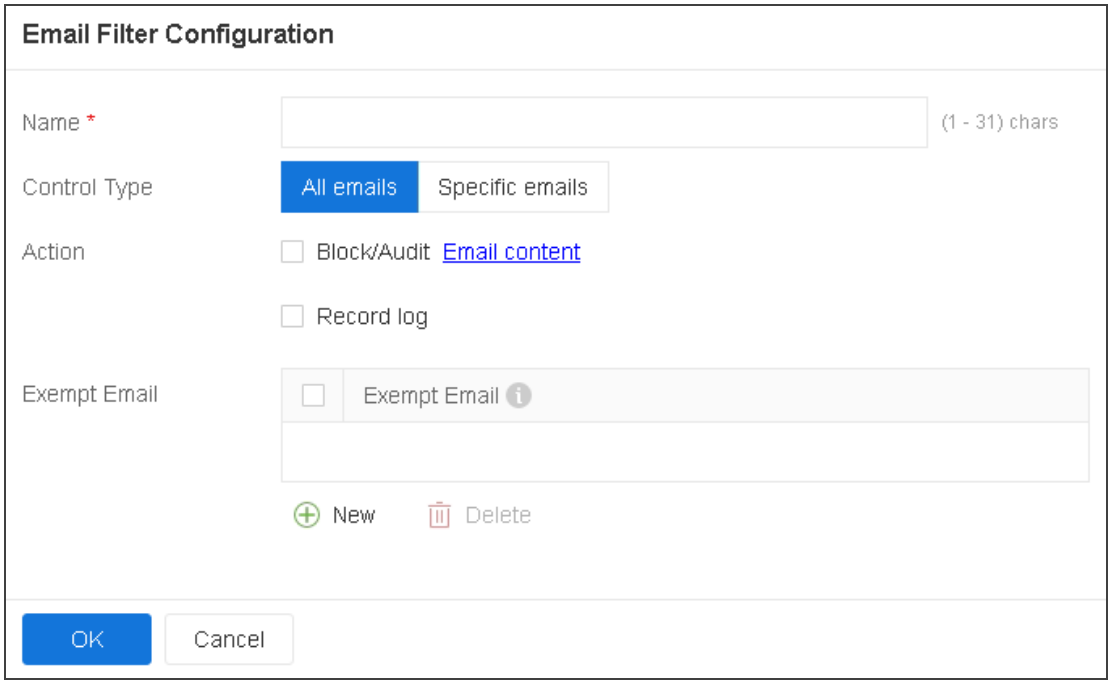
Configuring Email Filter

Configuring email filter contains two parts:

- Create an email filter rule
- Bind an email filter rule to a security zone or policy rule

Part 1: Creating an email filter rule

1. Select **Object > Data Security > Content Filter > Email Filtering Log**.
2. Click **New**.



Option	Description
Name	Specifies the rule name.
Control Type	All emails - This option applies to all the sending emails. • Record Log - Select this check box if you want all emails to be logged.
	Specific mail items - This option applies to specific mail items. To configure the email sender: 1. Click **Sender**. 2. In the prompt, enter sender's email address. 3. Click **Add**. 4. You may select to block the sender or keep a record. 5. Click **OK**. To configure the email receiver: 1. Click **Recipient**. 2. In the prompt, enter email receiver's email address. 3. Click **Add**. 4. You may select to block the receiver or keep a record. 5. Click **OK**. To configure the email content keywords: 1. Click **email content**. 2. In the prompt, click **Add**. See the Keyword Category

Other emails	Select an action for emails other than which are added above.

Option	Description
Exempt Email	
Exempt Email	To configure mail addresses that do not follow the regulations of email filter: 1. Click **Exempt Email**. 2. In the prompt, enter emails that do not obey email filter. 3. Click **Add**, and you can add more. 4. Click **OK**.

Part 2: Binding an Email filter rule to a security zone or security policy rule

The email filter configurations are based on security zones or policies.

- If a security zone is configured with the email filter function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the email filter function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the email filter configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based email filter:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 152.
2. In the Zone Configuration dialog, select Threat Protection tab.

3. Enable the threat protection you need, and select an email filter rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create an email filter rule, see Creating an email filter rule.

4. Click **OK** to save the settings.

To realize the policy-based email filter:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 1090.

2. In the Protection tab, select the **Enable** check box of email filter.

3. From the **Profile** drop-down list, select an email filter rule. You can also click **Add Profile** to create a new email filter rule.

4. Click **OK** to save the settings.

If needed, you can also configure SSL proxy, keyword category, warning page, bypass domain and user exempt user.

To configure those features, click **Configuration** on the right top corner of the Email Filtering Log list page.

Option	Description
Keyword Category	Use the keyword category function to customize the keyword categories. You can use it to specify the keyword for the URL category/Web posting/email filter functions.
Warning Page	• Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser. • Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
Exempt User	Users that are not controlled by the internet behavior control rules.

Notes:

- If an email filter rule has added all three of Audit/Block Sender, Receiver and email content, the rule will take effect when one of them is hit.
- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1602.
- By default, a rule will immediately take effect after you click **OK** to complete configuration.

Viewing Monitored Results of Email Keyword Blocking

If you have configured email filter with keyword blocking, you can view the monitored results of blocking those words.

Select **Monitor > Keyword Block > Email Content**, you will see the monitored results. For more about monitoring, refer to "Email Content" on Page 1540.

Viewing Logs of Emails Keyword Blocking

To see the system logs of email's keywords, please refer to the "Content Filter Log" on Page 1583.

APP Behavior Control

The APP behavior control function is designed to control and audit (record log messages) the actions of FTP, HTTP(S) and TELNET applications, including:

- Controlling and auditing the FTP content and Login, Get, and Put actions;
- Controlling and auditing the Connect, Get, Put, Head, Options, Post, Trace, Delete actions of HTTP(S);
- Controlling and auditing the request content initiated by TELNET client.

Configuring APP Behavior Control

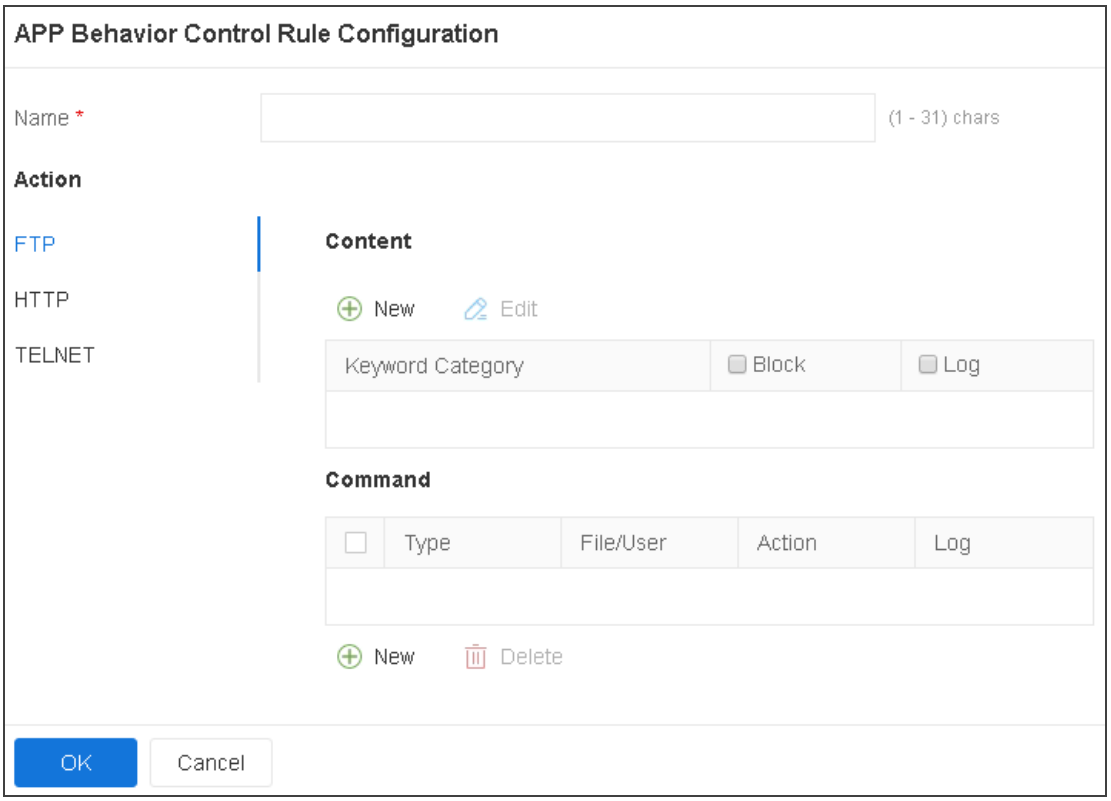
Configuring behavior control contains two parts:

- Creating an application behavior control rule
- Binding an application behavior control rule to a security zone or policy rule

Part 1: Creating an APP behavior control rule

1. Select **Object > Data Security > Content Filter > APP Behavior Control**.

2. Click **New**.



Option	Description
Name	Specifies the rule name.
Action	
FTP	Content: Controls the FTP content. If the content matches the specified keyword categories, system will execute the specified action, including **Block** or **Log**. Expand the **Content**, and configure the control options. • **New**: Click the button to create a keyword category. For how to create the category, refer to the Keyword Category of Configuring Objects. • **Edit**: Select one keyword from the list and edit the cat-

Option	Description
	egory. • **Keyword Category**: Displays the keyword categories in system. • **Block**: Select the check box to block the FTP content matching the keyword category. • **Log**: Select the check box to record logs when the FTP content matches the keyword category. Command: Controls the FTP methods, including Login, Get, and Put. Expand the **Command**, and configure the control options. • From the first drop-down list, select the method to be controlled, it can be GET, PUT, or Login. • Type the file name (for the method of GET or PUT) or user name (for the method of Login) into the next box. • From the second drop-down list, select the action. It can be Block or Permit. • From the third drop-down list, specify whether to record the log messages. • Click **Add**. • Repeat Step 1 to 5 to add more control entries. To edit/delete a control entry, select the entry from the list, and then click **Edit** or **Delete**.

Option	Description
HTTP	Comment: Controls the HTTP(S) methods, including Connect, GET, PUT, Head, Options, Post, Trace, and Delete. Expand HTTP(S), and configure the HTTP(S) control options. • From the first drop-down list, select the method to be controlled, it can be Connect, GET, PUT, Head, Options, Post, Trace, or Delete. • Type the domain name into the next box. • From the second drop-down list, select the action. It can be Block or Permit. • From the third drop-down list, specify whether to record the log messages. • Click **Add**. • Repeat Step 1 to 5 to add more control entries. To edit/delete a control entry, select the entry from the list, and then click **Edit** or **Delete**.
TELNET	Content: Controls the request content initiated by the TELNET client. If the content matches the specified keyword categories, system will execute the specified action, including **Block** or **Log**. Expand the **Content**, and configure the control options. • **New**: Click the button to create a keyword category. For how to create the category, refer to the Keyword Category of Configuring Objects. • **Edit**: Select one keyword from the list and edit the cat-

Option	Description
	egory. • **Keyword Category**: Displays the keyword categories in system. • **Block**: Select the check box to block the request content matching the keyword category. • **Log**: Select the check box to record logs when the request content matches the keyword category.

3. Click **OK**.

Part 2: Binding an APP behavior control rule to a security zone or security policy rule

The APP behavior control configurations are based on security zones or policies.

- If a security zone is configured with the APP behavior control function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the APP behavior control function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the APP behavior control configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based APP behavior control:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 152.

2. In the Zone Configuration dialog, select Data Security tab.
3. Enable the threat protection you need, and select an email filter rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create an APP behavior control rule, see Creating an APP behavior control rule.
4. Click **OK** to save the settings.

To realize the policy-based APP behavior control:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 1090.
2. In the Data Security tab, select the **Enable** check box of APP behavior control.
3. From the **Profile** drop-down list, select a APP behavior control rule. You can also click **Add Profile** to create a new APP behavior control rule.
4. Click **OK** to save the settings.

If necessary, you can configure some additional features by going to the right top corner and click **Configuration**.

Option	Description
Predefined URL database	The predefined URL database includes dozens of categories and tens of millions of URLs and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
User-defined URL database	The user-defined URL database is defined by yourself and you can use it to specify the URL category and URL range for the URL category/Web posting functions.
URL lookup	Use the URL lookup function to inquire URL information from the URL database.
Keyword category	Customizes keyword categories as needed.

Option	Description
Warning Page	• Block warning: When your network access is blocked, you will be prompted with a warning page in the Web browser. • Audit warning: When your network access is audited, you will be prompted with a warning page in the Web browser.
Bypass Domain	Domains that are not controlled by the internet behavior control rules.
Exempt User	Users that are not controlled by the internet behavior control rules.



Notes:

- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1602.
- By default, a rule will immediately take effect after you click **OK** to complete configuration.

Viewing Logs of APP Behavior Control

To see the system logs of APP behavior control, please refer to the "Content Filter Log" on Page 1583.

Network Behavior Record

Network behavior record function audits the IM applications behaviors and record log messages for the access actions, includes:

- Audits the QQ, WeChat and sinaweibo user behaviors.
- Log the access behaviors.

Configuring Network Behavior Recording

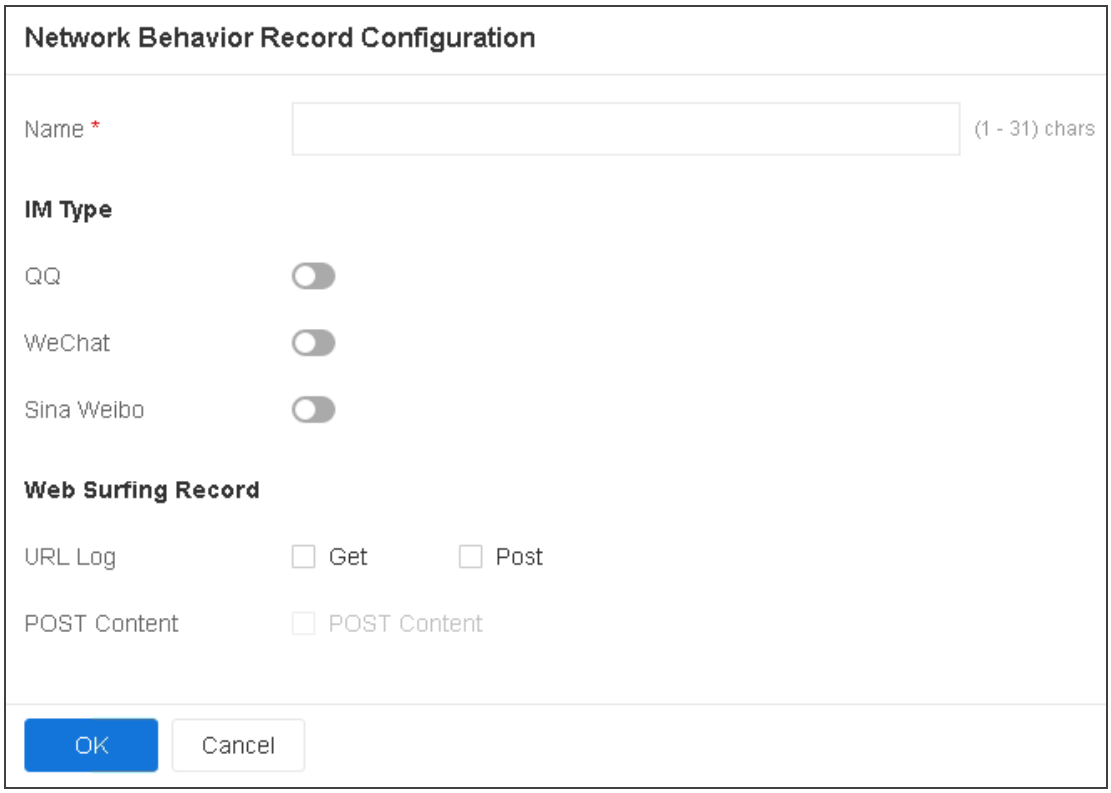
Configuring network behavior record contains two parts:

- Create a network behavior record rule
- Bind a network behavior record rule to a security zone or policy rule

Part 1: Creating a NBR rule

1. Select **Object > Data Security > Network Behavior Record**.

2. Click **New**.



Option	Description
Name	Specifies the rule name.
IM	
QQ	To audits the QQ behavior. 1. Select the **QQ** checkbox. 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 10. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs.

Option	Description
WeChat	To audits the WeChat behavior. 1. Select the **Wechat** checkbox. 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 20. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs.
Sina Weibo	To audits the sina weibo behavior. 1. Select the **Sina Weibo** checkbox 2. Timeout: Specifies the timeout value. The unit is minute. The default value is 20. During the timeout period, the IM user traffic of the same UID will not trigger the new logs and after the timeout reaches, it will trigger new logs.
Web Surfing Record	
URL Log	logs the GET and POST methods of HTTP. • Get: Records the logs when having GET methods. • Post: Records the logs when having POST methods.
POST Content	Post Content: Records the posted content.

3. Click **OK**.

Part 2: Binding a network behavior record rule to a security zone or security policy rule

The network behavior record configurations are based on security zones or policies.

- If a security zone is configured with the network behavior record function, the system will perform detection on the traffic that is destined to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the network behavior record function, the system will perform detection on the traffic that is destined to the policy rule you specified, and then response.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the network behavior record configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based network behavior record:

1. Create a zone. For more information about how to create, refer to "Security Zone" on Page 152.
2. In the Zone Configuration dialog, select Data Security tab.
3. Enable the threat protection you need, and select a network behavior record rules from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list below, to create a network behavior record rule, see Creating a network behavior record rule.
4. Click **OK** to save the settings.

To realize the policy-based network behavior record:

1. Configure a security policy rule. See "Configuring a Security Policy Rule" on Page 1090.
2. In the Data Security tab, select the **Enable** check box of network behavior record.
3. From the **Profile** drop-down list, select a network behavior record rule. You can also click

Add Profile to create a new network behavior record rule.

4. Click **OK** to save the settings.



Notes:

- You can export logs to a designated destination. Refer to "Log Configuration" on Page 1602
- By default, a rule will immediately take effect after you click **OK** to complete configuration

Viewing Logs of Network Behavior Recording

To see the logs of network behavior recording, please refer to the "Network Behavior Record Log" on Page 1584.

End Point Protection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The endpoint security control center is used to monitor the security status of each access endpoint and the system information of the endpoint.

When the end point protection function is enabled, the device can obtain the endpoint data monitored by the endpoint security control center by interacting with it, and then specify the corresponding processing action according to the security status of endpoint, so as to control the endpoint network behavior.



Notes:

- At present, end point protection function only supports linkage with "JIANGMIN" endpoint security control center.



- End point protection is controlled by license. To use end point protection, apply and install the EPP license.

Related Topics:

- "Configuring End Point Protection" on Page 1453
- "Configuring End Point Security Control Center Parameters" on Page 1458
- "End Point Monitor" on Page 1526
- "EPP Log" on Page 1581

Configuring End Point Protection

This chapter includes the following sections:

- Preparation for configuring end point protection function.
- Configuring end point protection function.

Preparing

Before enabling end point protection, make the following preparations:

1. Make sure your system version supports end point protection.
2. Import an EPP license and reboot.

Configuring End Point Protection Function

The end point protection configurations are based on security zones or policies.

To realize the zone-based end point protection, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. In the **Zone Configuration**page, select **End Point Protection** tab.
3. Enable the end point protection you need and select an end point protection rule from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list. To create an endpoint protection rule, see Configuring End Point Protection Rule.
4. Click **OK** to save the settings.

To realize the policy-based endpoint protection, take the following steps:

1. Create a security policy rule. For more information, refer to "Security Policy" on Page 1089.
2. In the Policy Configuration page, expand Protection.
3. Select the **Enable** check box of **End Point Protection**. Then select an endpoint protection rule from the Profile drop-down list, or you can click **Add Profile** from the Profile drop-down list to create an end point protection rule. For more information, see Configuring End Point Protection Rule.
4. Click **OK** to save the settings.



Notes: When the zone and policy bind the same end point protection rule, the priority is policy > zone.

Configuring End Point Protection Rule

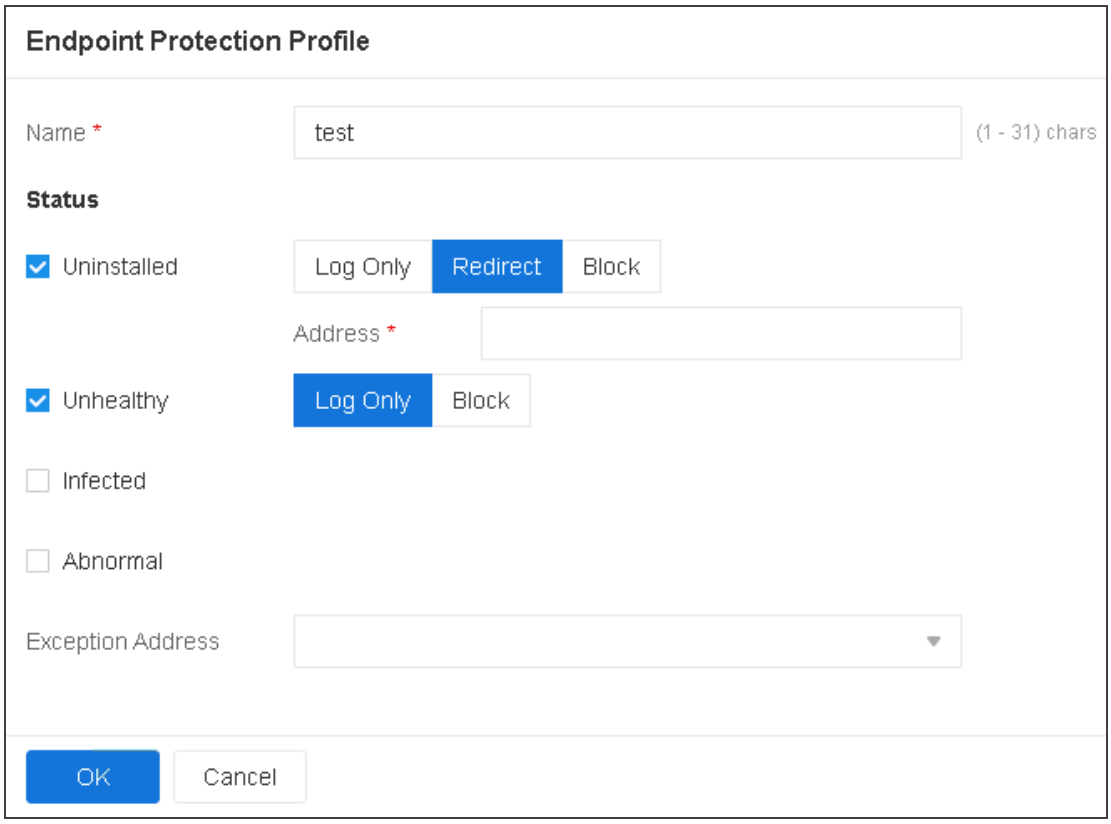
System has two default end point protection rules: **predef_epp** and **no_epp**.

- **predef_epp**: Execute the **Logonly** action for the endpoint whose status is "Uninstall" and "Unhealthy". Execute the **Block** action for the endpoint whose status is "Infected" and "Abnormal", and the block time is 60s.
- **no_epp**:No protective action is executed on all endpoints by default.

To configure an end point protection rule, take the following steps:

1. Click **Object> End Point Protection > Profile**.

2. Click **New**.



Option	Description
Name	Specifies the rule name.
Status	Specifies the protection action corresponding to the endpoint status. • Uninstalled: Specifies the protection action for the end-point which doesn't install an anti-virus client. Select the **Uninstalled** check box, and select the protection action in the drop-down list.

Option	Description
	• Redirect - Redirects the endpoint to the specified URL. Enter the URL in the **Address** text box. • Logonly - System will pass traffic and record logs only. • Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. The unit is second. The value ranges from 60 to 65535. • Unhealthy: Specifies the protection action for the unhealthy endpoint. Select the **Unhealthy** check box, and select the protection action in the drop-down list. • Logonly - System will pass traffic and record logs only. • Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. The unit is second. The value ranges from 60 to 65535. • Infected: Specifies the protection action for the infected endpoint. Select the **Infected** check box, and select the protection action in the drop-down list. • Logonly - System will pass traffic and record logs only.

Option	Description
	• Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. The unit is second. The value ranges from 60 to 65535. • Abnormal: Specifies the protection action for the abnormal endpoint. Select the **Abnormal** check box, and select the protection action in the drop-down list. • Logonly - System will pass traffic and record logs only. • Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. The unit is second. The value ranges from 60 to 65535.
Exception Address	The exception address is not controlled by the end point protection rule. Select the address book name in the drop down list. **Notes:** Before selecting the exception address, you need to add the exception endpoint address to the address book. For configuration, see "Address" on Page 814.

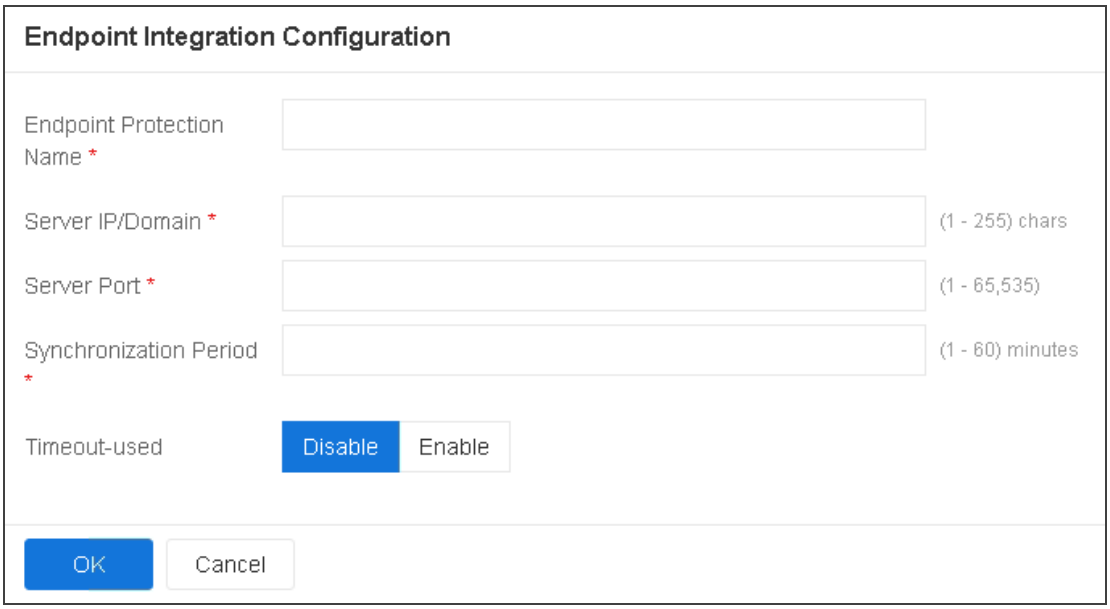
3. Click **OK** to save the settings.

Configuring End Point Security Control Center Parameters

To configure the endpoint security control center parameters, take the following steps:

1. Go to **System > Third Party Linkage**.

2. Click **New**.



Option	Description
Endpoint Prevention Name	Display the end point protection type as Jiangmin. Only one endpoint security control center server with the same type can be configured.
Server IP/Domain	Specifies the address or domain name of the endpoint security control center server. The range is 1 to 255 characters.
Server Port	Specifies the port of the endpoint security control center server. The range is 1 to 65535.
Synchronization Period	Specifies the synchronization period of endpoint data information. The range is 1 to 60 minutes. The default value is 10 minutes.
Timeout-used	• Disable: When the endpoint security control center is disconnected with the device and doesn't restore to

Option	Description
	connection in two synchronization periods, the synchronized endpoint data information will be cleared. By default, the timeout entry is disabled. • Enable: When the endpoint security control center is disconnected with the device and doesn't restore to connection in two synchronization periods, the endpoint data information that the system has been synchronized the last time continues to be used.

3. Click **OK**.

ACL

System supports ACL (Access Control List) based on MAC addresses and DSCP. You can create access control profile based on MAC addresses and bind the profile to security policies to achieve access control of the specific MAC addresses and DSCP. With the combination of security policy and ACL rules, system can achieve accurate access controlling.

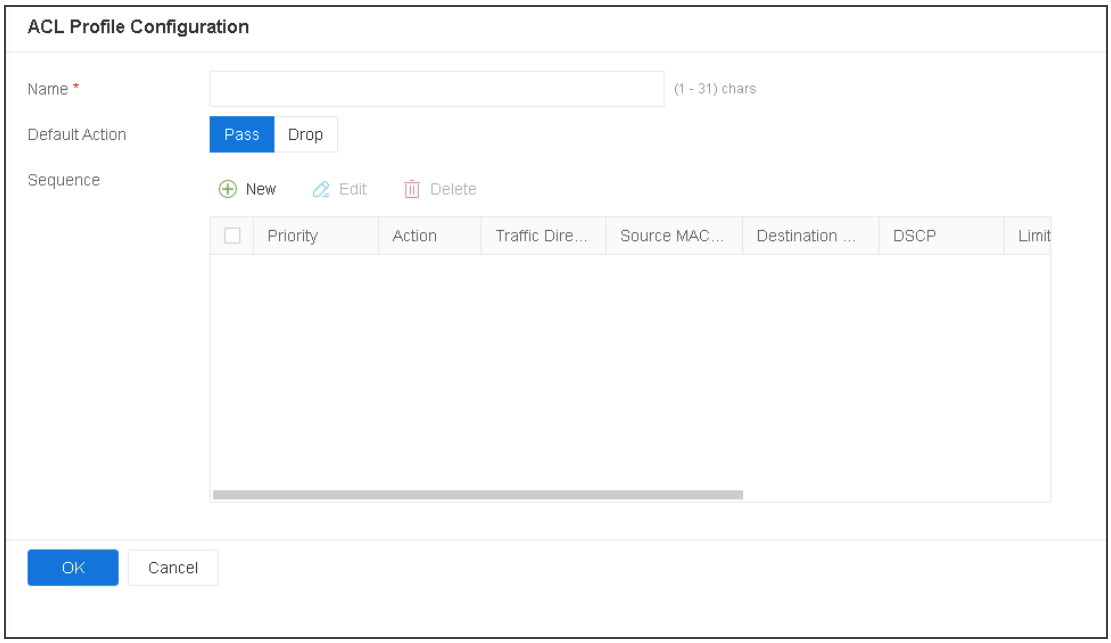
ACL Profile

The ACL profile consists of one or more access control rules. In the access rule, you can set the source MAC address and destination MAC address and DSCP to filter the packets flowing through the device, and set access control action for the matched packets, pass or discard. The configured access control profiles will take effect only when they are bound to security policies.

To configure an ACL profile, take the following steps:

1. Select **Object** > **ACL** > **Profile**.

2. Click **New** and the ACL Profile Configuration dialog box will appear.

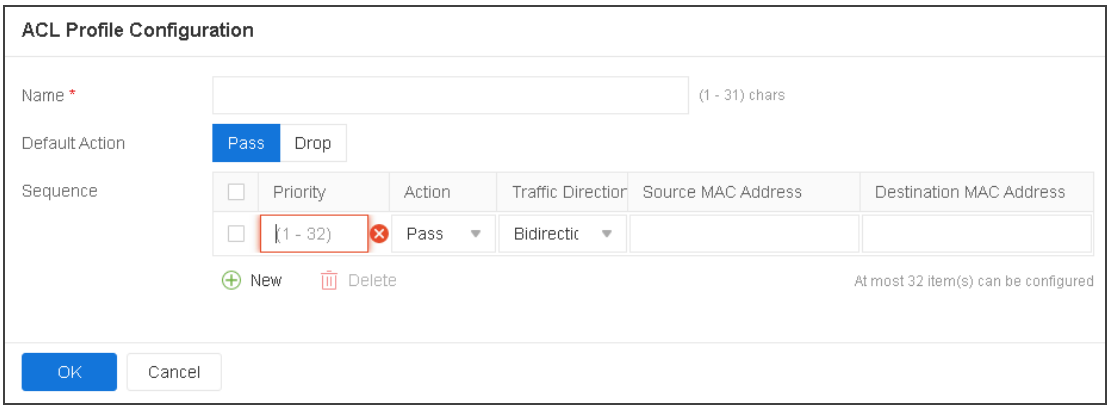


In the ACL Profile Configuration dialog, configure the corresponding options.

Option	Description
Name	Specify the name of the ACL profile.
Default Action	Specify the default action of access control. For the packets which match the access control rule in the list below, it will be processed according to the action set in the access control rule; for the packets which fail to match the access control rule, it will be processed according to the default action set here. Default control actions include: • Pass: By default, packets will be allowed to pass the detection of access control, but still need to

Option	Description
	be detected via IPS, Anti-virus and so on. • Block: By default, packets will be blocked directly and will not pass through the device.

3. Click New on the ACL Profile Configuration, and the ACL Rule Configuration dialog pops up.



In the <ACL Rule Configuration> dialog, configure the corresponding options.

Option	Description
Priority	Specify the priority of ACL rules to be matched, ranging from 1 to 32. The bigger the value, the higher the priority.
Action	Specify the action to be executed after the ACL rules have been matched, including: • Pass: Packets will be allowed to pass the detection of access control, but still need to be detected via IPS, Anti-virus and so on. • Block: Packets will be blocked directly and will not pass through the device.

Option	Description
Traffic Direction	Specify the traffic direction of the ACL rule. **Forward** indicates the traffic direction where the session is initiated. **Backward** indicates traffic direction where the session is responded. **Bidirectional** indicates the direction of both Forward and Backward. By default, system matches the bidirectional traffic.
Source MAC Address	Specify the source MAC address of packets to be matched.
Destination MAC Address	Specify the destination MAC address of packets to be matched.
DSCP	Specify the DSCP value to be matched. The range is 0-63.
Limit Type	Specify the limit type that the access control rules match for the extension headers of IPv6 messages, including Total Header Number, Single Header Number and Header Order.
	• Total Header Number: Select this option and then specify the Total Header Number and Comparison Mode. The system will count and limit the total number of extension headers in IPv6 message. If the restriction requirements are met, the system will process according to the action of this rule. • Single Header Number: Select this option, and then specify the Header and Comparison Mode. The system will count and limit the specify header in IPv6 message. If the restriction requirements are met, the system will process according to the action of this rule.

Option	Description
	• Header Order:Select this option, and then specify the Header Order:Positive Sequence and out of order.Positive Sequence means that the extension headers should be arranged in order. " Out of order" means that the extension headers are arranged in non order, that is, out of order. If the restriction requirements are met, the system will process according to the action of the rule.
Log	System will log when the messages matching the access control rules.

4. Click **OK**.

Honeypot

Introduction

Hillstone Deception Decoy System employs deception and trap techniques to induce and redirect malicious traffic, leading attackers into a honeypot environment. This disrupts their tactics, consumes their time, actively combats their actions, and provides you with proactive defense capabilities, including attack capture, attack display, attacker profiling, attack replay, data analysis, and traceback and countermeasures. The deception decoy system acts as the last line of defense.

The system supports the honeypot function and enables collaboration between the firewall device and Hillstone Deception Decoy System (Honeypot or Honeypot system). By connecting the honeypot system to the firewall device and configuring trap rules, attacker IP addresses that match the trap rules are diverted to the honeypot system for containment. This prevents attacks on your real business environment. Meanwhile, the honeypot system analyzes trapped attacker information, synchronizes it to the firewall device, and then allows you to add attacker IP addresses to the blacklist based on your requirements.

Configuring the Honeypot Function

To configure the Honeypot function, take the following steps:

1. Connecting to Honeypot
2. Configuring a Trap Rule
3. Viewing and Handling the Threat Information about Attackers

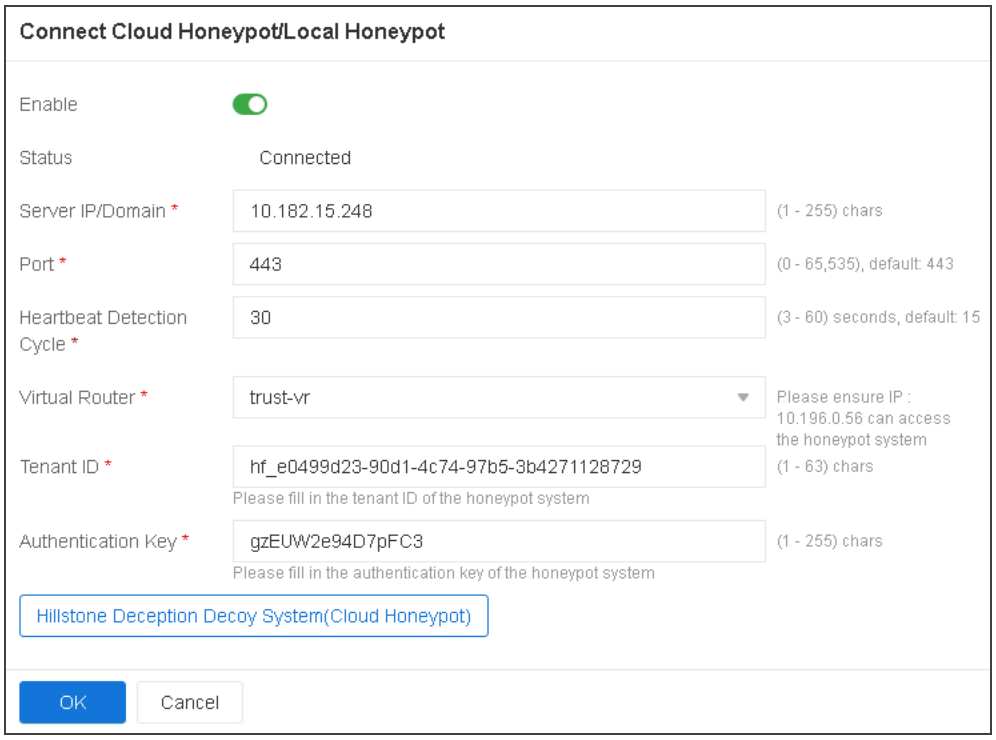
Connecting to Honeypot

Before you use the Honeypot function, the firewall needs to connect to the honeypot system (including cloud honeypot or local honeypot). Before the connection, you need to obtain the following information about the honeypot system: IP address or domain name of the server, port number, tenant ID, and authentication key. After the connection is established and the authentication is successful, the firewall sends heartbeat messages to the honeypot system at regular intervals to check the connection.

To connect to Honeypot, take the following steps:

1. Select **Object** > **Honeypot** > **Configuration**.

2. Turn on the switch next to Enable and configure the following options:



Option	Description
Status	Displays the connection status between the firewall and honeypot system, including **Connected** and **Disconnected**.
Server IP/Domain	Enter the IP address or domain name of the server of the honeypot system, which needs to be 1 to 255 characters in length.
Port	Enter the port number of the honeypot system. Valid values: 0 to 65535. Default value: 443.
Heartbeat Detection Cycle	The heartbeat detection cycle is used to check the connection between the firewall and honeypot system. If the firewall does not receive a heartbeat message from the honeypot system

Option	Description
	within the specified heartbeat detection cycle, the firewall and honeypot are not connected. Enter a heartbeat detection cycle. Valid values: 3 to 60 seconds. Default value: 15 seconds.
Virtual Router	Select the virtual router to which the honeypot system belongs from the drop-down list.
Tenant ID	Enter the tenant ID of the honeypot system. This ID is provided by the honeypot system. To obtain this ID, contact Hillstone technical support.
Authentication Key	Enter the authentication key of the honeypot system. This key is provided by the honeypot system. To obtain this key, contact Hillstone technical support.

3. Click **OK**.

To enter the honeypot system, click Hillstone Deception Decoy System(Cloud Honeypot) to quickly access the login page of the WebUI of this system.

Configuring a Trap Rule

The system can divert the attack traffic to the decoy business of the honeypot based on the conditions configured in the trap rule. This ensures the security of real business.

To configure a trap rule, take the following steps:

1. Select **Object** > **Honeypot** > **Trap Rules**.

2. Click **New** and configure the following options:



Option	Description
Rule Name	Enter the name of the trap rule, which needs to be 1 to 127 characters in length.
IP Type	Sets the IP type to IPv4 or IPv6. This parameter is available only when the system version is IPv6.
Source Address	When the IP type is set to IPv4, enter the IPv4 address and subnet mask of the attacker. When the IP type is set to IPv6, enter the IPv6 address and prefix length of the attacker.
Disguised Address	When the IP type is set to IPv4, enter the disguised IPv4 address and subnet mask. When the IP type is set to IPv6, enter the disguised IPv6 address and prefix length. If the attacker access the disguised IP address, the trap rule is

Option	Description
	hit.
Honeypot Template	After the firewall establishes a connection with the honeypot system, honeypot templates in the honeypot system will be automatically synchronized to the firewall. The attacker who hits the trap rule will be diverted to the disguised business of the honeypot template. This protects your real business from attacks. Select a honeypot template from the drop-down list. To view details about the template, click .
Virtual Router	Select the virtual router to which the effective scope of the trap rule belongs. If not specified, the trap rule takes effect globally.

3. Click **OK**.

Notes: You can create at most 255 trap rules.

In the trap rule list, after you select a trap rule, you can perform the following operations:

- Click **Edit** in the upper part of the list to edit the specified trap rule.
- Click **Delete** in the upper part of the list to delete the specified trap rule.
- Click **Enable** in the upper part of the list to enable the specified trap rule.
- Click **Disable** in the upper part of the list to disable the specified trap rule.

Viewing and Handling the Threat Information about Attackers

The honeypot system analyzes trapped attacker information and synchronizes it to the firewall device. On the Threat Information page, you can view threat information about attackers, includ-

ing the IP address of the attacker, threat level, and country/region. You can also add the attacker IP address to the blacklist based on your requirements.

To view and handle the threat information about attackers, take the following steps:

1. Select **Object** > **Honeypot** > **Threat Information**. On this page, view the threat information about attackers, including the attack source IP address, threat level, country/region, start time, and end time.
2. Click + to the left of a threat information entry. On the victim information page, view in formation about the corresponding victim, including the destination IP address, honeypot name, threat tag, service type, trap address partition, and remarks.
3. For the attacker IP address that you want to handle, click in the **Add Blacklist** column in the threat information list or click **Add Blacklist** in the upper part of the victim information list. This way, you can add the attacker IP address to the blacklist and configure the time during which the attacker IP address is blocked. After the attacker IP address is added to the blacklist, the system blocks the IP address until the block period expires. For more information about the blacklist, see Configuring a Dynamic IP Blacklist.

Chapter 11 Policy

The Policy module provides the following functions:

- Security policy: Security policy the basic function of devices that are designed to control the traffic forwarding between security zones/segments. By default all traffic between security zones/segments will be denied.
- NAT: When the IP packets pass through the devices or routers, the devices or routers will translate the source IP address and/or the destination IP address in the IP packets.
- QoS: QoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. QoS can assure the normal transmission of critical business traffic when the network is overloaded or congested.
- Session limit: The session limit function limits the number of sessions and controls the session rate to the source IP address, destination IP address, specified IP address, service, or role/user/user group, thereby protecting from DoS attacks and control the bandwidth of applications, such as IM or P2P.
- Perimeter Traffic Filtering: It can filter the perimeter traffic based on known IP of black-/white list, and take block action on the malicious traffic that hits the blacklist.

Security Policy

Security policy is the basic function of devices that is designed to control the traffic forwarding between security zones/segments. Without security policy rules, the devices will deny all traffic between security zones/segments by default. After configuring the security policy rule, the device can identify what traffic between security zones or segments will be permitted, and the others will be denied.

The basic elements of policy rules:

- The source zone and address of the traffic
- The destination zone and address of the traffic
- The service type of the traffic
- Actions that the devices will perform when processing the specific type of traffic, including Permit, Deny, Tunnel, From tunnel, WebAuth, and Portal server.

Generally a security policy rule consists of two parts: filtering conditions and actions. You can set the filtering conditions by specifying traffic's source zone/address, destination zone/address, service type, and user. Each policy rule is labeled with a unique ID which is automatically generated when the rule is created. You can also specify a policy rule ID at your own choice. All policy rules in system are arranged in a specific order. When traffic flows into a device, the device will query for policy rules by turn, and processes the traffic according to the first matched rule.

The max global security policy rule numbers may vary in different models.

Security policy supports IPv4 and IPv6 address. If IPv6 is enabled, you can configure IPv6 address entry for the policy rule.

This section contains the following contents:

- Configure a security policy rule
- Manage the security policy rules: enable/disable a policy rule, clone a policy rule, adjust security rule position, configure default action, view and clear policy hit count, hit count check,

rule redundancy check, importing /exporting policy rule searching policy rules and configure policy audit function.

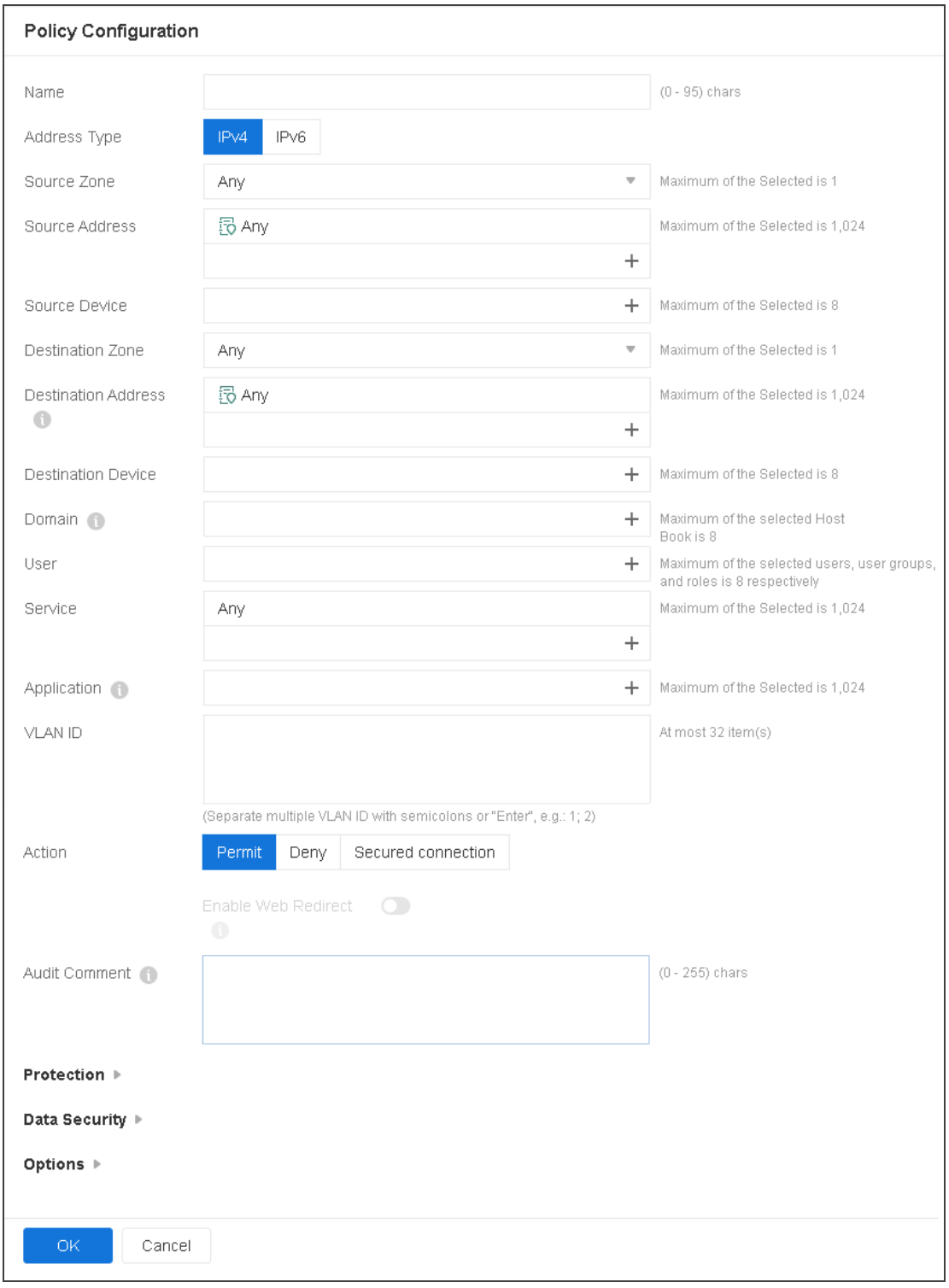
- Configure an aggregate policy
- Configure a security policy group
- Configure a mini policy
- View and search the security policy rules/ security policy groups
- Configure the policy assistant

Configuring a Security Policy Rule

To configure a security policy rule, take the following steps:

1. Select **Policy > Security Policy > Policy**.

2. At the top-left corner, click **New** to open the **Policy Configuration** page.



Configure the corresponding options.

Option	Description
Name	Type the name of the security policy.
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware can configure the IPv6 type. If IPv6 is selected, all of the IPv6/prefix, IP range, and addressbook should be configured in the IPv6 format.
Source Zone	Specifies a source zone. In the single-zone mode, select a zone from the **Source Zone** dropdown list. If the multi-zone mode is enabled, take the following steps: 1. Click **Source Zone** to go to the pop-out Zone list. 2. Click the zones you need. You can select up to 16 zones. 3. Click **OK**. You can also perform the following operations: • When selecting the zones, you can click ⊕ to create new zones. • Any is the default zone. Enable **Any**to restore to the default.
Source Address	Specifies the source addresses. 1. Click **Address** to select an address type from the **Address** dialog.

Option	Description
	2. Select or type the source addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close** to complete the source address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ icon to create a new address entry. • You can click ▼ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be

Option	Description
	matched. • The default address configuration is any. Enable **Any** to restore the configuration to this default one.
Source Device	Specifies the source device of the policy rule. 1. Click **Source Device**. The dialog box displays existing device objects. 2. Select one or more device objects. At most 8 device objects can be selected. 3. Click **Close**. You can also perform the following operations: • When you select a device object, you can click  to create one. • When you select a device object, you can click in the search box to search for device objects by device name, manufacturer, type, model, OS family, and OS version.
Destination Zone	Specifies a destination zone. In the single-zone mode, select a zone from the **Destination Zone** dropdown list. If the multi-zone mode is enabled, take the following steps: You can also perform the following operations: • When selecting the zones, you can click  to create new

Option	Description
	zones. • Any is the default zone. Enable **Any** to restore to the default.
Destination Address	Specifies the destination addresses. 1. Click **Address** to select an address type from the **Address** dialog. 2. Select or type the destination addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close** to complete the destination address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ icon to create a new address entry. • You can click ▼ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the

Option	Description
	address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • The default address configuration is any. Enable **Any** to restore to the default.
Destination Device	Specifies the destination device of the policy rule. 1. Click **Destination Device**. The dialog box displays existing device objects. 2. Select one or more device objects. At most 8 device objects can be selected. 3. Click **Close**. You can also perform the following operations: • When you select a device object, you can click ⊕ to create one. • When you select a device object, you can click ▼ in the search box to search for device objects by device name, manufacturer, type, model, OS family, and OS version.

Option	Description
Domain	Specifies the domain/host book. The domain, destination address, and application cannot be configured at the same time. 1. Click **Domain**, select a type: Domain, Host Book. 2. Select a domain/host book to add it to the left pane. • If Domain is selected, you need to enter a domain name and click **Add**. At most 1,024 domain names can be added. • If Host Book is selected, you can select a host book. At most 8 host books can be added. You can also search for host books based on keyword or click  to create a host book. 3. After adding the desired domains/host books, click **Close**. Note: After you specify the domain/host book, the policy rule is not used for redundancy check.
User	Specifies a role, user or user group for the security policy rule. 1. Click **User** to select the AAA server where the users and user groups reside. To specify a role, select **Role** from the **AAA Server/Role** drop-down list. 2. Based on the type of AAA server, you can execute one or more actions: search a user/user group/role, expand the user/user group list, enter the name of the user/user

Option	Description
	group. 3. After selecting users/user groups/roles, click the selected users/user groups/roles to add them to the left pane. 4. After adding the desired objects, click **Close** to complete the user configuration.
Service	Specifies a service or service group. 1. From the **Service** drop-down menu, select a type: Service, Service Group. 2. You can search the desired service/service group, expand the service/service group list. If Service is selected, you can click next to the search box to filter services by keyword, name, and protocol type of service. 3. After selecting the desired services/service groups, click the selected services/service groups to add them to the left pane. 4. After adding the desired objects, click **Close** to complete the service configuration. You can also perform other operations: • To add a new service or service group, click icon.

Option	Description
	• The default service configuration is any. Enable **Any** to restore to the default. Specifies a service rule. When configuring the service rule of the policy rule, you can add a predefined or user-defined service that have been configured in the service book. When the required service does not exist in the service book, the administrator can specify the protocol type and port number of the service by configuring the service rules, thus simplifying the configuration steps of the policy. Specify a protocol type for the user-defined service. The available options include TCP, UDP, ICMP, SCTP and Others. If needed, you can add multiple service items. The parameters for the protocol types are described as follows: 1. From the **Service** drop-down menu, select a type: Service Rule. 2. From the **Protocol Type**drop-down menu, select a protocol type: TCP, UDP, ICMP, ICMPv6 and All. The parameters for the protocol types are described as follows: **TCP/UDP**: • Destination port: • Min - Specifies the minimum port number of the specified service rule.

Option	Description
	• Max - Specifies the maximum port number of the specified service rule. The value range is 0 to 65535. • Source port: • Min - Specifies the minimum port number of the specified service rule. • Max - Specifies the maximum port number of the specified service rule. The value range is 0 to 65535.  Notes: • The minimum port number cannot exceed the maximum port number. • The "Min" of the destination port is required, and other options are optional. • If "Max " is not configured, system will use "Min" as the single code. ICMP: • Type: Specifies an ICMP type for the service rule.

Option	Description
	The value range is 0（Echp-Reply）, 3（Destination-Unreachable）, 4（Source Quench）, 5（Redirect）, 8（Echo）, 11（Time Exceeded）, 12（Parameter Problem）, 13（Timestamp）, 14（Timestamp Reply）, 15（Information Request）, 16（Information Reply）, 17（Address Mask Request）, 18（Address Mask Reply）, 30（Traceroute）, 31（Datagram Conversion Error）, 32（Mobile Host Redirect）, 33（IPv6 Where-Are-You）, 34（IPv6 I-Am-Here）, 35（Mobile Registration Request）, 36（Mobile Registration Reply）. • Code: Specifies a minimum value and maximum value for ICMP code. The value range is 0 to 15, the default value is : min code - 0, max code - 15. Notes: • The minimum code cannot exceed the maximum code. • If "Max " is not configured, system will use "Min" as the single code. ICMPv6:

Option	Description
	• Type: Specifies an ICMPv6 type for the service rule. The value range is 1（Dest-Unreachable）, 2（Packet Too Big）, 3（Time Exceeded）, 4（Parameter Problem）, 5-99 (Unallocated Error message), 100（Private experimentation）, 101（Private experimentation）, 102-126 (Unallocated Error message), 127（Reserved for expansion of ICMPv6 error message）, 128（Echo Request）, 129（Echo Reply）, 130（Multicast Listener Query）, 131（Multicast Listener Report）, 132（Multicast Listener Done）, 133（Router Solicitation）, 134（Router Advertisement）, 135（Neighbor Solicitation）, 136（Neighbor Advertisement）, 137（Redirect Message）, 138（Router Renumbering）, 139（ICMP Node Information Query）, 140（ICMP Node Information Response）, 141（Inverse Neighbor Discovery Solicitation Message）, 142（Inverse Neighbor Discovery Advertisement Message）, 143（Version 2 Multicast Listener Report）, 144（Home Agent Address Discovery Request Massage）, 145（Home Agent Address Discovery Reply Massage）, 146（Mobile Prefix Solicitation）, 147（Mobile Prefix Advertisement ）, 148（Cer-

Option	Description

	tification Path Solicitation Message）, 149（Certification Path Advertisement Message）, 150（ICMP message utilized by experimental mobility protocols such as Seamoby）, 151（Multicast Router Advertisement）, 152（Multicast Router Solicitation ）, 153（Multicast Router Termination）, 154（FMIPv6 Messages）, 200（Private experimentation）, 201（Private experimentation）and 255（Reserved for expansion of ICMPv6 informational）.
	• Code: Specifies a minimum value and maximum value for ICMP code. The value range is 0 to 255, the default value is : min code - 0, max code - 255.
	SCTP:
	• Destination port
	  • Min- Specifies the minimum port number of the specified service rule.
	  • Max- Specifies the maximum port number of the specified service rule. The value range is 0 to 65535.
	• Source port
	  • Min - Specifies the minimum port number

Option	Description
	of the specified service rule. • Max - Specifies the maximum port number of the specified service rule. The value range is 0 to 65535. Notes: • The minimum port number cannot exceed the maximum port number. • The "Min" of the destination port is required, and other options are optional. • If "Max " is not configured, system will use "Min" as the single code. ALL: • Protocol: Specifies a protocol name for the service rule. If it is a unknown protocol, you can directly enter the corresponding protocol number. . Notes: • The minimum code cannot

Option	Description
	 exceed the maximum code. • If "Max " is not configured, system will use "Min" as the single code. 3. Click **Add** to add the configured service rules to the list on the left. 4. Click **Close** .
Application	Specifies an application/application group/application filters. 1. Click **Application**, in the pop-up dialog, you can search the desired application/application group/application filter, expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click the selected applications/application groups/application filters to add them to the left pane. 3. After adding the desired objects, click **Close** to complete the application configuration. You can also perform other operations: • To add a new application group, select **Application Groups** from the **Application** drop-down menu and click

Option	Description
	icon. • To add a new application filter, select **Application Filters** from the **Application** drop-down menu and click icon. **Note**: Deprecated predefined applications cannot be added.
VLAN ID	Specifies the VLAN ID that is matched to the policy rule. The value range is from 1 to 4,094. If multiple VLAN IDs are specified, separate them with semicolons. Each policy rule supports up to 32 VLAN IDs.

Action	Specifies an action for the traffic that is matched to the policy rule, including:
	• Permit - Select **Permit** to permit the traffic to pass through.
	• Deny - Select **Deny** to deny the traffic.
	• Secured Connection:
	  • WebAuth - Performs Web authentication on the matched traffic. Select **WebAuth** from the drop-down list after selecting the **Secured Connection** option, and then select an authentication server from the following drop-down list.
	  • From tunnel (VPN) - For the traffic from a peer to local, if this option is selected, system will first determine if the traffic originates from a tunnel.

Option	Description
	Only such traffic will be permitted. Select **From tunnel (VPN)** from the drop-down list after selecting the **Secured Connection** option, and then select a tunnel from the following drop-down list. • Tunnel (VPN) - For the traffic from local to a peer, select this option to allow the traffic to pass through the VPN tunnel. Select **Tunnel (VPN)** from the drop-down list after selecting the **Secured Connection** option, and then select a tunnel from the following drop-down list. To allow traffic from this specified VPN tunnel at the same time, select **Bi-directional policy**. When the policy rule is created, another policy rule with the **From tunnel (VPN)** field set to this VPN tunnel will be automatically created. **Note**: The Bi-directional VPN Policy function can be configured only when you create a policy rule. • Portal server - Performs portal authentication on the matched traffic. Select **Portal server** from the drop-down list after selecting the **Secured Connection** option, and then type the URL address of the portal server.
Enable Web Redirect	Enable the Web redirect function to redirect the HTTP request from clients to a specified page automatically. With this function

Option	Description
	enabled, system will redirect the page you are requesting over HTTP to a prompt page. 1. Click the **Enable Web Redirect** button. 2. Type a redirect URL into the **Notification page URL** box. When using Web redirect function, you need to configure the Web authentication function. For more configurations, see "User Online Notification" on Page 1177.
Audit Comment	After the "Configuration Audit" function is enabled, this option is required when creating or modifying a policy, and you must add policy audit comments to the text box. The range is 1 to 255 characters. For detailed operation of this function, please refer to Configuring Policy Audit Function. When the "Configuration Audit" function is not enabled, this option is optional and the range is 0 to 255 characters. For enabling/disabling the "Configuration Audit" function, please configure it in the **Option** page (**System > Device Management > Option**), refer to the Configuration Audit.

Expand Protection, configure the corresponding options.

Option	Description
Antivirus	Specifies an antivirus profile. The combination of security policy rule and antivirus profile enables the devices to implement fine-grained application layer policy control.

Option	Description
IPS	Specifies an IPS profile. The combination of security policy rule and IPS profile enables the devices to implement fine-grained application layer policy control.
URL Filtering	Specifies a URL filter profile. The combination of security policy rule and URL filter profile enables the devices to implement fine-grained application layer policy control.
Sandbox	Specifies a sandbox profile. The combination of security policy rule and sandbox profile enables the devices to implement fine-grained application layer policy control.
Botnet Prevention	Specifies a botnet prevention profile. The combination of security policy rule and botnet prevention profile enables the devices to implement fine-grained application layer policy control.

Expand Data Security, configure the corresponding options.

Option	Description
File Filter	Specifies a file filter profile. The combination of security policy rule and file filter profile enables the devices to implement fine-grained application layer policy control.
File Content Filter	Specifies a file content filter profile. The combination of security policy rule and file content filter profile enables the devices to implement fine-grained application layer policy control.
File Content Filter	Specifies a file content filter profile. The combination of security policy rule and file content filter profile enables the devices to implement fine-grained application layer policy control.

Option	Description
Web Content	Specifies a web content profile. The combination of security policy rule and Web Content profile enables the devices to implement fine-grained application layer policy control.
Web Posting	Specifies a web posting profile. The combination of security policy rule and web posting profile enables the devices to implement fine-grained application layer policy control.
Email Filter	Specifies an email filter profile. The combination of security policy rule and email filter profile enables the devices to implement fine-grained application layer policy control.
APP Behavior Control	Specifies an app behavior control profile. The combination of security policy rule and app behavior control profile enables the devices to implement fine-grained application layer policy control.
Network Behavior Record	Specifies a NBR profile. The combination of security policy rule and NBR profile enables the devices to implement fine-grained application layer policy control.

Expand Options, configure the corresponding options.

Option	Description
Schedule	Specifies a schedule when the security policy rule takes effect. Select a desired schedule from the **Schedule** dialog. This option supports fuzzy search. After selecting the desired schedules, click the blank area in this page to complete the schedule configuration. To create a new schedule, click ⊕ icon.
Session	Specifies the session timeout period of the policy rule. The ses-

Option	Description
Timeout	sion timeout period indicates the aging period of session in the policy rule. After the timeout period is reached, the session is disconnected. Valid values: 1 to 65535 seconds or 1 to 1000 days.
Log	You can log policy rule matching in the system logs according to your needs. • For the policy rules of Permit, logs will be generated in two conditions: the traffic that is matched to the policy rules starts and ends its session. • For the policy rules of Deny, logs will be generated when the traffic that is matched to the policy rules is denied. Select one or more check boxes to enable the corresponding log types. • Deny - Generates logs when the traffic that is matched to the policy rules is denied. • Session start - Generates logs when the traffic that is matched to the policy rules starts its session. • Session end - Generates logs when the traffic that is matched to the policy rules ends its session.
SSL Proxy	Specifies a SSL proxy profile. The combination of security policy rule and SSL proxy profile enables the devices to decrypt the HTTPS traffic.
Policy Assist-	Click the **Enable** button to enable policy assistant. After

Option	Description
ant	enabling the policy assistant, you can specify the policy ID as the traffic hit policy. System can analyze the traffic data hit the specified policy ID, and aggregate the traffic list according to the user-defined aggregation rules, and finally the security policy rules that meet your expectations can be generated. For how to use policy assistant, see Configuring the Policy Assitant.
ACL	Click the **Enable** button to enable the access control function and select the ACL profile. With the combination of security policy and ACL rules, system can achieve accurate access controlling.
Aggregate Policy	Click the Aggregate Policy drop-down menu, and select the aggregate policy to be added to the aggregate policy to which you want to add.
Position	Select a rule position from the Position drop-down list. Each policy rule is labeled with a unique ID or name. When traffic flows into a device, the device will query for the policy rules by turn, and processes the traffic according to the first matched rule. However, the policy rule ID is not related to the matching sequence during the query. The sequence displayed in policy rule list is the query sequence for policy rules. The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name.
Description	Type descriptions into the **Description** box.

Click Userdefined Attribute and enter the corresponding configuration.

Option	Description
User-defined Attributes 1-8	Specifies the custom attribute content of the policy, which can be up to 31 characters in length. You can use custom attributes to filter policy rules, which helps you query and manage policies. **Note**: For more information about how to filter policy rules by custom policy rule attributes, see Filtering Policy Rules by Using Custom Policy Rule Attributes.

3. Click **OK** to save your settings.

Managing Security Policy Rules

Managing security policy rules include the following matters: enable/disable a policy rule, clone a policy rule, adjust security rule position, configure default action, view and clear policy hit count, hit count check, and rule redundancy check.

Enabling/Disabling a Policy Rule

By default the configured policy rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a policy rule:

1. Select **Policy > Security Policy > Policy**.
2. Select the security policy rule that you want to enable/disable.
3. Click ⋮ icon , and then select **Enable** or **Disable** to enable or disable the rule.

The disabled rule will not display in the list. Click ⋮ icon , and then select **Show Disabled Policies** to show them.

Cloning a Policy Rule

When there are a large number of policy rules in system, to create a policy rule which is similar to an configured policy rule easily, you can copy the policy rule and paste it to the specified location.

To clone a policy rule, take the following steps:

1. Select **Policy > Security Policy > Policy**.
2. Select the security policy rule that you want to clone and click **Copy**.
3. Click **Paste**. In the drop-down list, select the desired position. Then the rule will be cloned to the desired position.

Adjusting Security Policy Rule Position

To adjust the rule position, take the following steps:

1. Select **Policy > Security Policy > Policy**.
2. Select the check box of the security policy whose position will be adjusted.
3. Click **Move**.
4. In the drop-down list, type the rule ID or name , and click **Top**, **Bottom**, **Before ID** , **After ID** , **Before Name** ,or **After Name**. Then the rule will be moved to the top, to the bottom, before or after the specified ID or name.

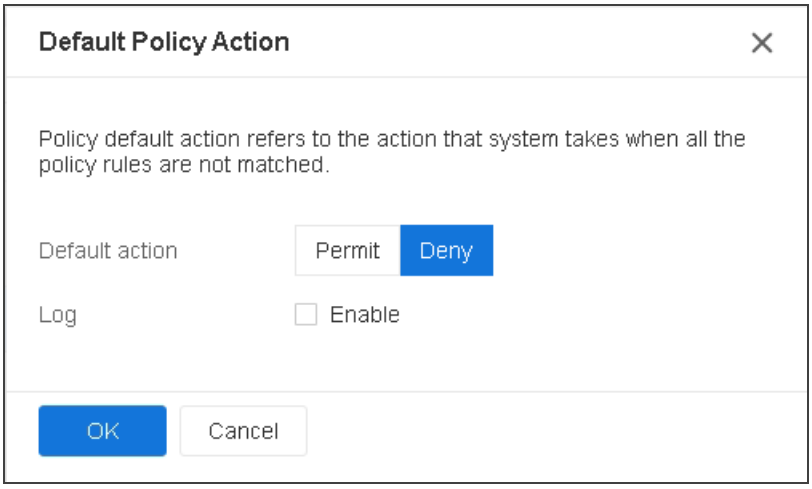
Configuring Default Action

You can specify a default action for the traffic that is not matched with any configured policy rule. System will process the traffic according to the specified default action. By default system will deny such traffic.

To specify a default policy action, take the following steps:

1. Select **Policy > Security Policy > Policy**.

2. Click ⋮ icon and select **Default Policy Action**.



Configure the following options.

Option	Description
Default action	Specify a default action for the traffic that is not matched with any configured policy rule. • Click **Permit** to permit the traffic to pass through. • Click **Deny** to deny the traffic.
Log	Configure to generate logs for the traffic that is not matched with any configured policy rule. By default system will not generate logs for such traffic. To enable log, click the **Enable** button, and system will generate logs for such traffic.

3. Click **OK** to save your changes.

Filtering Policy Rules by Using Custom Policy Rule Attributes

To facilitate policy query and management and query, you can configure custom attributes for policy rules and filter policy rules based on custom attributes.

Custom attributes greatly facilitate administrators in filtering, categorizing, and querying policies. For example, in a company where the network administrator has deployed thousands of policies and is not fully aware of the usage of certain policies, custom attributes can be used to clearly view information such as the user and expiration date of the current policy. By configuring a custom attribute for the policy as 'User' and setting the 'User' in the policy rule to 'Zhang San,' you can quickly filter and find policy rules where the user is 'Zhang San' by using 'Zhang San' as the filter condition.

The procedure is as follows:

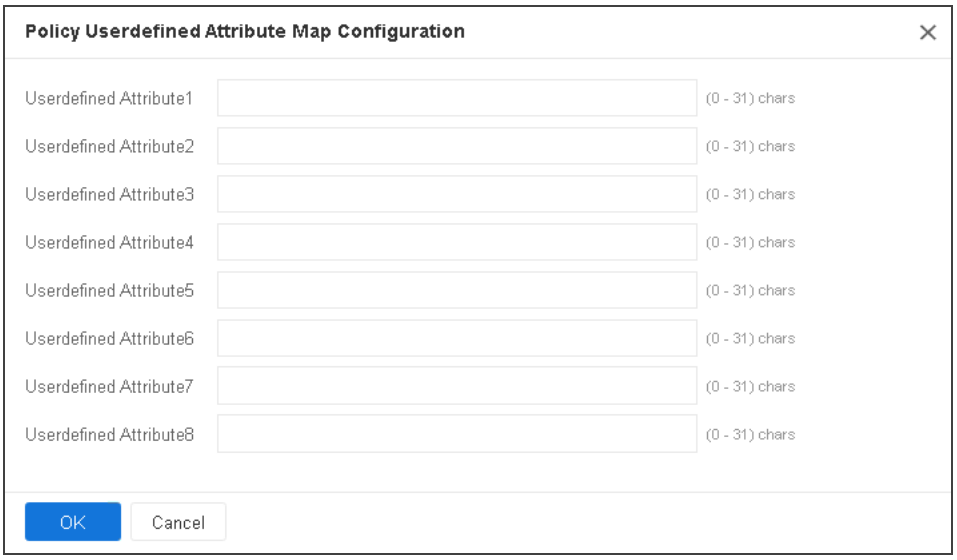
1. Configure custom attributes mapping
2. Configure custom attributes for policy rules
3. Filter policy rules

Take the following steps:

Step 1: Configure custom attributes mapping

1. Select **Policy** > **Security Policy** > **Policy**.
2. Click ⋮ and select **Policy Userdefined Attribute Map Configuration**.
3. In the "Userdefined AttributeX" field, enter the custom policy attribute. In the following figure, "Userdefined Attribute 1" is set to "User" and "Userdefined Attribute 2" is set to

"Department".



4. Click **OK**.

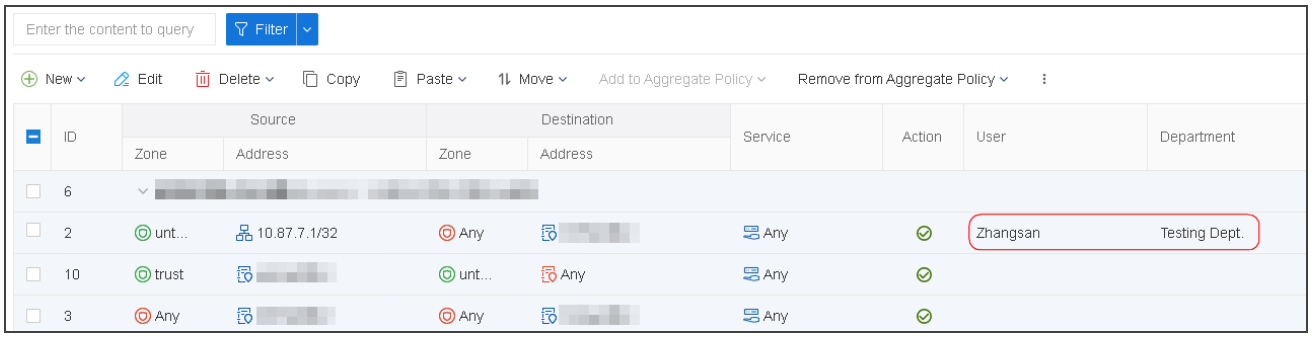
Step 2: Configure custom attributes for policy rules

1. Click **New** or **Edit**.
2. In the **Userdefined Attribute** section, the attributes configured in Step 1 are displayed. In this example, "User" and "Department" are displayed.



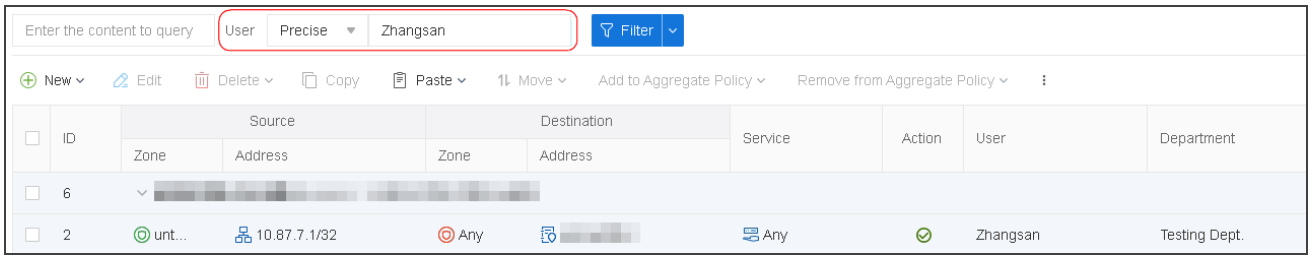
3. Enter Zhangsan for "User" and Testing Dept. for "Department".

4. Click **OK**. Then, the user and department are displayed in the policy rule list.



Step 3: Filter policy rules

1. On the policy rule list page, click Filter in the upper-left corner, select "User" as the filter condition, and then enter "Zhangsan".



2. All policy rules whose "User" is "Zhangsan" are displayed in the list.

Policy Global Configuration

The global configuration of policies includes:

- Switching between multi-zone and single-zone
- Security Policy Matching Destination Addresses After DNAT
- Enabling/Disabling traffic statistics of policies
- Enabling/Disabling the Delay Address Update Time Function

Switching between Multi-zone and Single-zone

In the Policy Global Configuration, you can switch to multi-zone or single-zone mode. In the single-zone mode, one policy supports only one source zone and one destination zone. In the multi-zone mode, one policy supports multiple zones. In this case, users can manage policies more easily when there are fewer policies needed configuring in the system. By default, the system applies the single-zone mode.

To switch to multi-zone or single-zone mode, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Click ⋮ and select **Policy Global Config** to go to the **Policy Global Config** page.
3. Enable **Multi Zone**. If you disable multi-zone mode, the system switches to the single-zone mode.
4. Click **OK**.

Security Policy Matching Destination Addresses After DNAT

In the policy global configuration, you can configure that policies will be matched by destination addresses before or after DNAT. By default, security policies will be matched by destination addresses before DNAT.

To configure that policies will be matched by destination addresses after DNAT, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.
2. Click ⋮ to select **Policy Global Config** from the popped up panel.
3. Turn on the switch after **Match after DNAT** to enable this feature. In this case, the security policy will be matched according to the destination address after DNAT. Turn off the switch after **Match after DNAT** to disable this feature. In this case, the security policy will

be matched according to the destination address before DNAT.

4. Click **OK**.

Enabling/Disabling Traffic Statistics of Policies

The Traffic Statistics function of policies can be used to collect statistics of the system traffic that hits policy rules, including the number of upstream packets, the number of downstream packets, the number of upstream bytes, and the number of downstream bytes. By default, the Traffic Statistics function is disabled.

To enable/disable the Traffic Statistics function of policies, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.
2. Click ⋮ and select **Policy Global Config**.
3. Turn on the switch next to **Traffic Statistics**.
4. Click **OK**.

Enabling/Disabling the Delay Address Update Time Function

The system supports the Delay Address Update Time function. After you modify multiple addresses in the address book at a time, the system does not immediately synchronize the modified addresses to the policy referencing the address book. Instead, synchronization occurs after a specified delay period. This avoids slow configuration deployment due to frequent updates in address book members. By default, the Delay Address Update Time function is disabled.

To enable/disable the Delay Address Update Time function, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.
2. Click ⋮ and select **Policy Global Config**.
3. Turn on the switch next to **Delay Address Update Time** to enable this function and specify the delay time. Valid values: 1 to 3 seconds. After you enable this function, if an address in

the address book referenced by a policy changes, the system does not immediately synchronize the modified address to the policy. Instead, synchronization occurs after the specified delay time.

To disable this function, turn off the switch next to Delay Address Update Time.

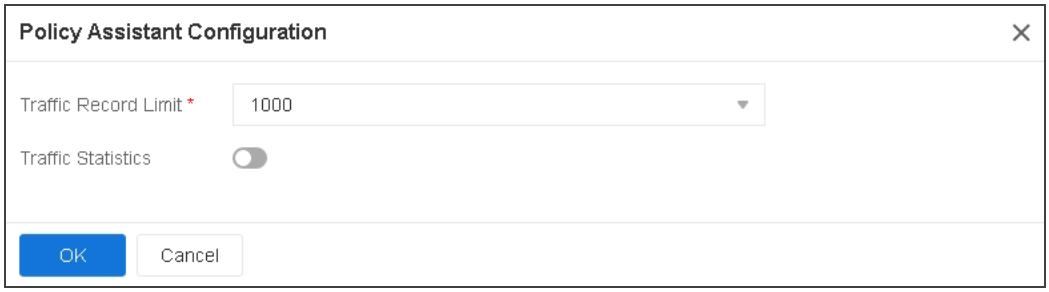
4. Click **OK**.

Enabling Traffic Statistics of Policy Assistant

The Traffic Statistics function of Policy Assistant can be used to collect statistics of the traffic extracted by Policy Assistant, including the number of hits, the number of upstream packets, the number of downstream packets, the number of upstream bytes, and the number of downstream bytes. By default, the Traffic Statistics function is disabled.

To enable the Traffic Statistics function of Policy Assistant, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.
2. Click ⋮ and select **Policy Assistant Configuration**.



3. In the **Policy Assistant Configuration** panel, turn on the switch next to **Traffic Statistics**.
4. Click **OK**.

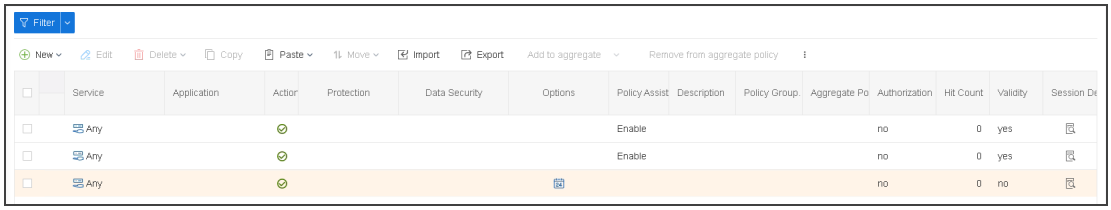
Schedule Validity Check

In order to make sure that the policies based on schedule are effective, system provides a method to check the validity of policies. After checking the policy, the invalid policies based on schedule

will be highlighted by yellow.

To check schedule validity:

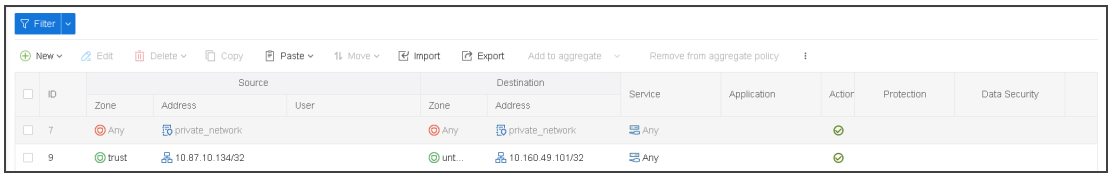
1. Select **Policy > Security Policy > Policy** .
2. Click ⋮ icon and select **Schedule Validity Check**. After check, system will highlight the invalid policy based on schedule by yellow. Meanwhile, you can view the validity status in the policy list.



Showing Disabled Policies

To show disabled policies:

1. Select **Policy > Security Policy > Policy** .
2. Click ⋮ icon and select **Show Disabled Policies**. The disabled policies will be highlighted by gray in the policy list.



Notes:

- By default(the "Schedule Validity Check" and "Show Disabled Policies" are not selected), the policy list only displays the enabled policies which are not

highlighted.

- When you select both "Schedule Validity Check" and "Show Disabled Policies", the policy is managed as follows:
  - The policy list will display the "Validity" column, which shows the validity status of policies.
  - The invalid policy based on schedule will be highlighted by yellow no matter if the policy is disabled or not.
  - If the valid policy based on schedule is disabled, it will be highlighted by gray.

Importing Policy Rule

You can import the configuration file of the local policy rules into the device to avoid creating policy rules manually. Only the DAT format file is supported currently.

To import the configuration file of policy rules, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Click the **Import** button to open the **Import** page.



3. Click **Browse** and select the local configuration file of policy rule to upload.

4. Click **OK**, and the imported policy rule will be displayed in the list.

> Notes:
>
> - If there's an error during import, system will stop importing immediately and roll back configurations automatically.
> - The imported policy will be displayed on the bottom of the policy list.

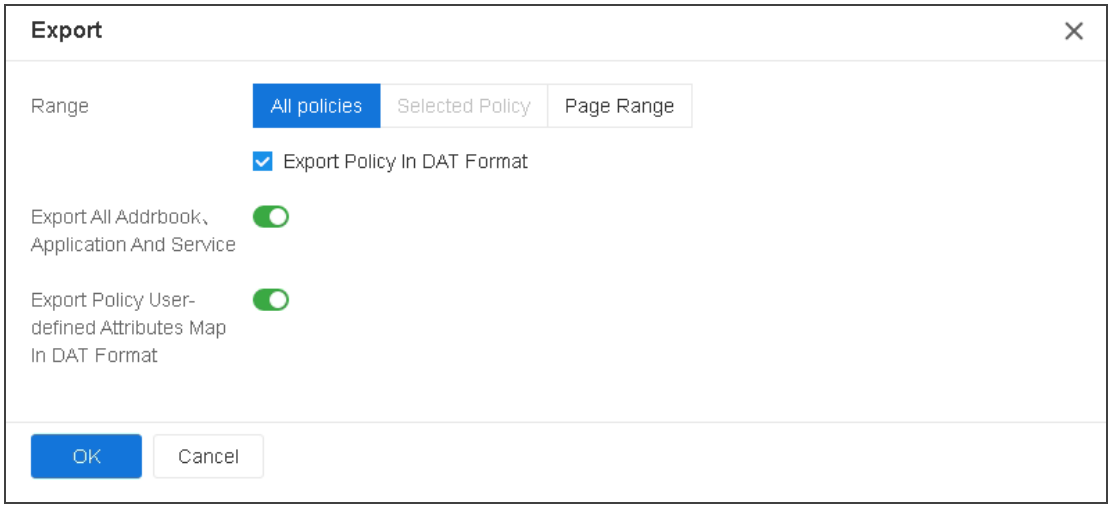
Exporting Policy Rule

You can export the policy rules existing on the device to the local in the format of HTML or DAT formats. At the same time, all the custom objects such as address book, service book and application can be exported.

To export the policy rules, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.

2. Click **Export** to open the **Export** page.

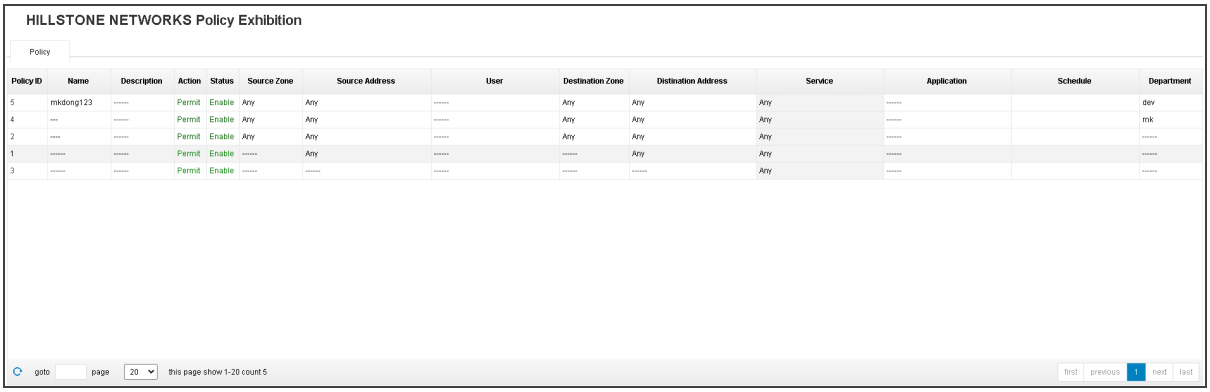


Configure the options as follows:

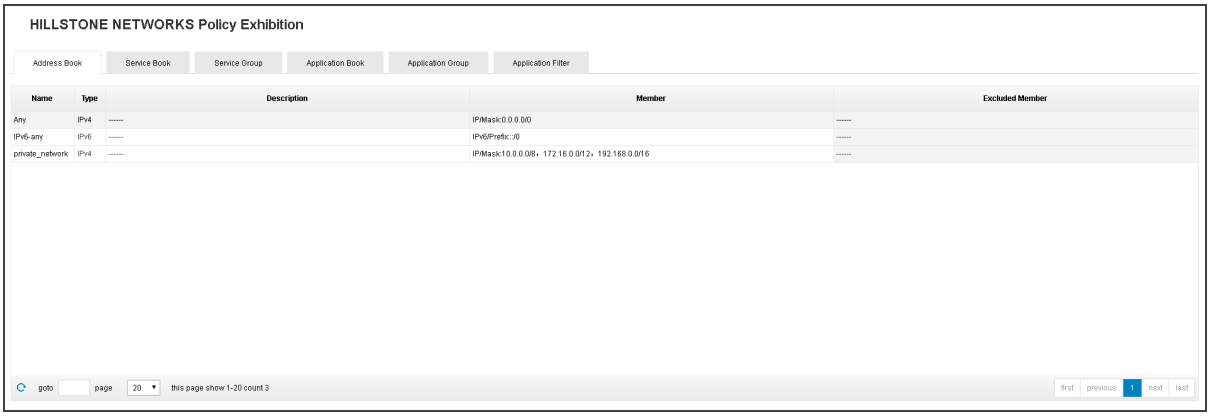
Option	Description
Range	Specify the range of policy rules to be exported. • All Policy: Select the radio button and export all policy rules on the device. • Selected Policy: In the policy list, select the policy to be exported, and then click **Export** > **Selected Policy**. • Page Range: Select the radio button, and enter the page number or page range of the policy list to be exported. **Note**: Separate the page number or range with semicolons, e.g. "3;5-8".
Export Policy in DAT Format	Select the check box to export the policy configurations in the format of DAT.
Export Address, Service, APP Book	Turn on the switch to export all the custom objects including address book, service book and application book, and a Zip file named "book+-exported time" will be generated.
Export Policy User-defined Attributes Map in DAT Format	Turn on the switch to export the custom attributes of the policy rules in the format of DAT.

3. Click **OK** to download the exported files. There're five kinds of files: policyExport.html, " policy+exported time.zip", "book+exported time.zip", policy configurations in the DAT format, and policy user-defined attributes file in the DAT format.

4. Double-click the policyExport.html, click **Import File** and import the " policy+exported time.zip" to view the table of exported policies.



5. Double-click the policyExport.html, click **Import File** and import the "book+exported time.zip" to view the table of object configurations.

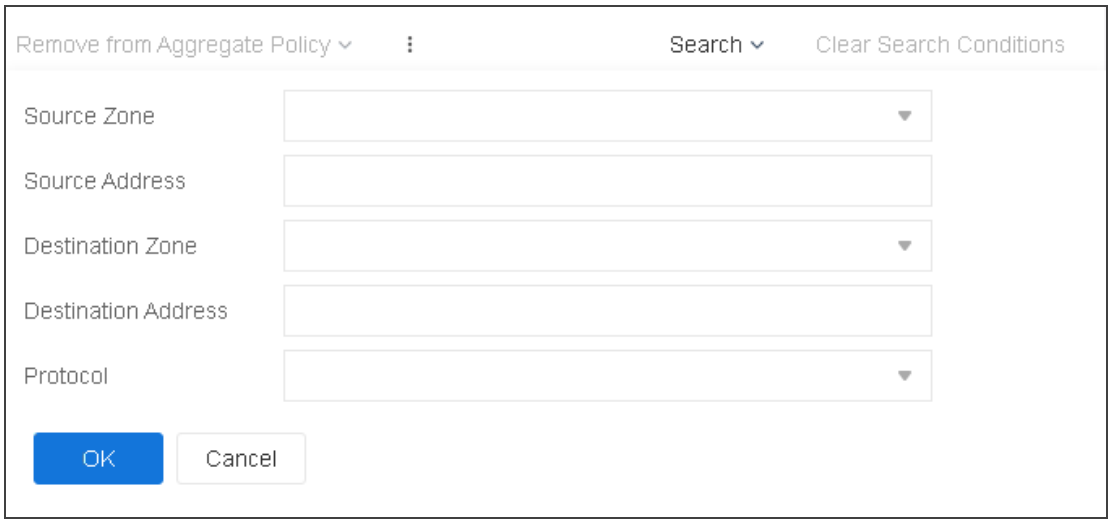


Searching Policy Rule

You can view the detailed information of the policy matching the five-tuple filtering conditions (including source IP address, destination IP address, protocol, source port and destination port), take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.

2. Click **Search** to open the configuration page.



Configure the options as follows:

Option	Description
Source Zone	Click the drop-down list to select the specified source zone, and search the policy rules that comply with the specified source zone.
Source Address	Enter the source address in the text box to search the policy rules that comply with the specified source address. The source address supports fuzzy matching, and can search the policy rules containing the input address.
Destination Zone	Click the drop-down list to select the specified destination zone, and search the policy rules that comply with the specified destination zone.
Destination Address	Enter the source address in the text box to search the policy rules that comply with the specified destination address. The

Option	Description
	destination address supports fuzzy matching, and can search the policy rules containing the input address.
Protocol	Select the protocol type in the **Protocol** drop-down list to search the policy rules that comply with the specified protocol. • When the protocol is specified as TCP or UDP, you can specify the source/destination port range, the value range is 0-65535, if you specify the same minimum and maximum source/destination port number, system will use this port number as the single source/destination port number. • When the protocol is specified as ICMP, the type and code range can be specified. If you specify the same minimum and maximum code value, the system will use the code value as a single code value. The value range of the code is 0-15. • When the protocol is specified as ICMPv6, the type and code range can be specified. If you specify the same minimum and maximum code value, the system will use the code value as a single code value. The value range of the code is 0-255. • When the protocol is specified as another protocol type, it does not support configuring the port range or code range.

Option	Description
	Note: If you specify a port range or code range, the maximum port number/code value and the minimum port number/code value must be configured at the same time.

3. Click the **OK**, the list will display the search results.

4. If you need to clear the configuration and display all the policy rules, click **Clear Search Conditions**.



Notes: The search function and the filter conditions are mutually exclusive and cannot be configured at the same time. When the search function is configured, the filter condition configuration will be cleared, and vice versa.

Configuring Policy Audit Function

System support the policy audit function. When you create or modify the policy rule/aggregate policy, you can use this function to add policy audit comments of the policy rule/aggregation policy so that you can understand the change reasons and change history of the policy rule/aggregate policy.



Notes: The policy audit function is available only for :

- SG-6000 A-Series devices installed with hard disks (excluding SG-6000-A1605/A1805/A2205).

For details about whether the device supports hard disks, see the Hardware Reference Guide.

Enabling the Configuration Audit Function

By default, the configuration audit function is disabled. To enable this function, take the following steps:

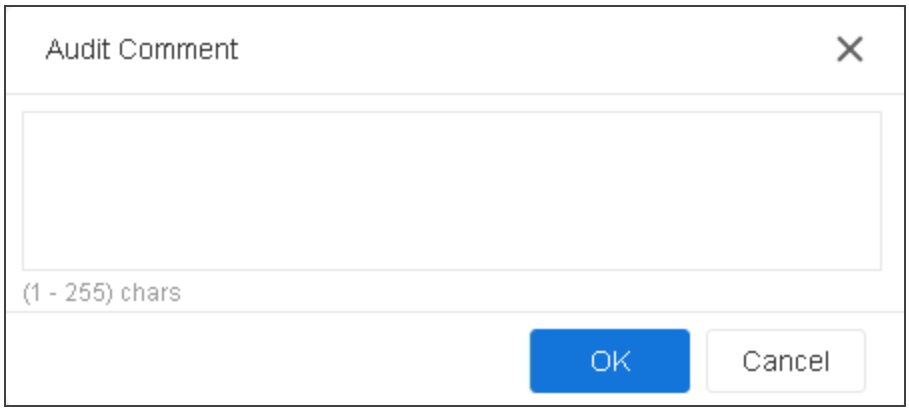
1. Select **System > Device Management > Option**.
2. In the System Setting page, select the **Enable** button for **Configuration Audit**, and click **OK**.

Adding the Audit Comment

When you create or modify the a policy rule/aggregate policy, you can add policy audit comments to the policy rule/aggregate policy, take the following steps:

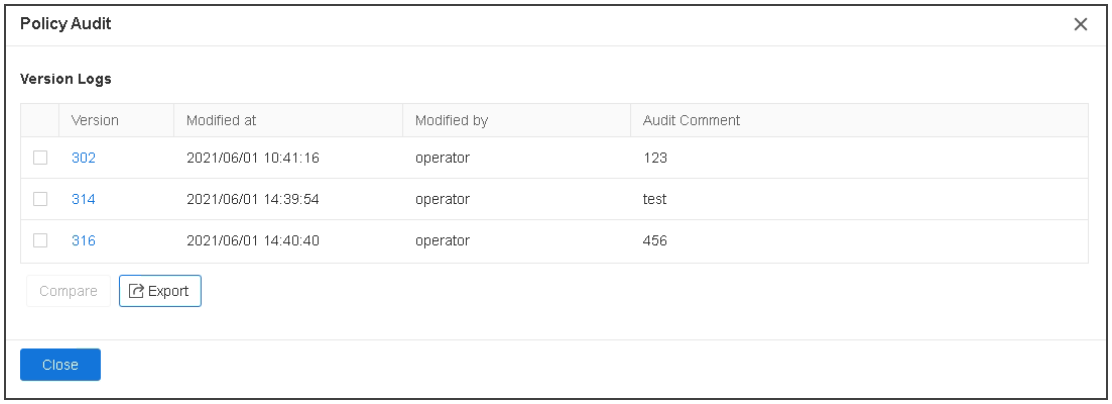
1. Click **Policy** > **Security Policy** > **Policy**.
2. Click the **New** drop-down list, and select **Policy** or **Aggregate Policy**, or select the policy rule/aggregate policy that needs to be edited in the list, and click the **Edit**.
3. In the **Audit Comment** text box in the **Policy Configuration** page, enter the content of the comment.
4. Click **OK**.

After deleting, pasting, moving, enabling, disabling the policy rule/aggregate policy, adding to the aggregation policy, and removing from the aggregate policy, the **Audit Comment** dialog box will pop up, and you need to fill in the comment content in the dialog box.



Viewing audit history

Under the **Audit Comment** text box in the **Policy Configuration** page, click the **Version Logs** to open the **Policy Audit** page to view the audit history of policy rules/aggregate policies.

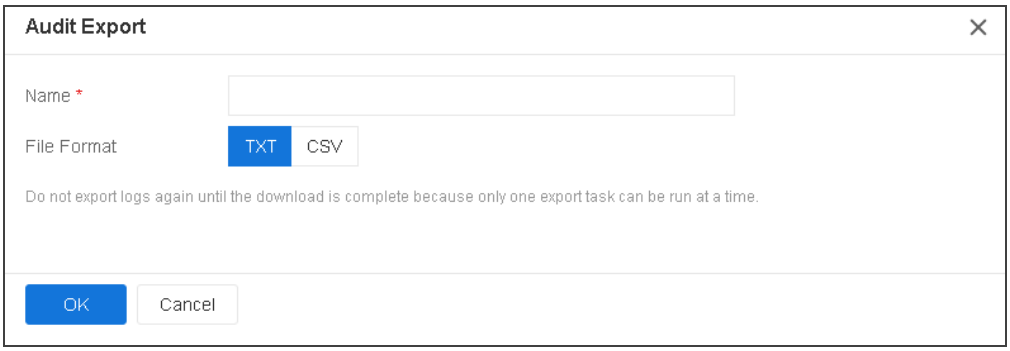


- In the **Version Logs** list, the version number, modification date, modification name, and audit comment content of the selected policy rule/aggregate policy are displayed. Among them, the **Version** is automatically assigned by system, and it will re-overlay from 1 after restoring the factory settings.
- Click the version number to open the Policy Configuration Details page to view the detailed configuration information of the policy.
- Select the two items that need to be compared and click **Compare**. The Results page below displays the content of the policy configuration information of the two versions, and the different content is highlighted in yellow.



- Select the item, click the **Export**, specify the name of the exported file and the type of export file format (TXT or CSV) in the **Audit Export** page, and then click **OK** and the browser will

launch the default download tool to download the export file compression package.



Notes: Only the system administrator (**admin**) support to export the audit history files.

Enabling Traffic Statistics of Policy Assistant

The Traffic Statistics function of Policy Assistant can be used to collect statistics of the traffic extracted by Policy Assistant, including the number of hits, the number of upstream packets, the number of downstream packets, the number of upstream bytes, and the number of downstream bytes. By default, the Traffic Statistics function is disabled.

To enable the Traffic Statistics function of Policy Assistant, take the following steps:

1. Select **Policy** > **Security Policy** > **Policy**.
2. Click ⋮ and select **Policy Assistant Configuration**.



3. In the **Policy Assistant Configuration** panel, turn on the switch next to **Traffic Statistics**.

4. Click **OK**.

Configuring an Aggregate Policy

According to the needs of different scenarios, you can create an aggregate policy, and add some policy rules with the same effect or the same attributes to the aggregation policy. If the administrator adjusts the position of an aggregate policy, the positions of all its members will be adjusted accordingly, so as to manage policy rules in bulk.

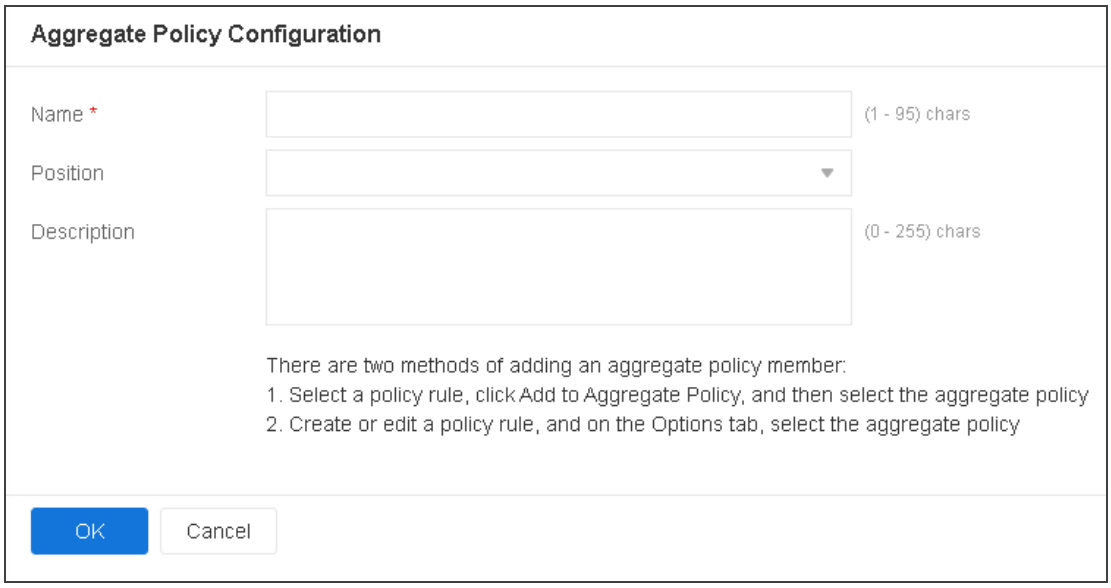
Configuring an aggregate policy includes: creating an aggregate policy, adding an aggregate policy member, removing an aggregate policy member, deleting an aggregate policy, adjusting the position of an aggregate policy, and enabling/disabling an aggregate policy.

Creating an Aggregate Policy

To create an aggregate policy, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.

2. Click the **New** drop-down list, and select **Aggregate Policy** to open the **Aggregate Policy Configuration** page .



On the Aggregate Policy Configuration tab, complete the basic configuration information.

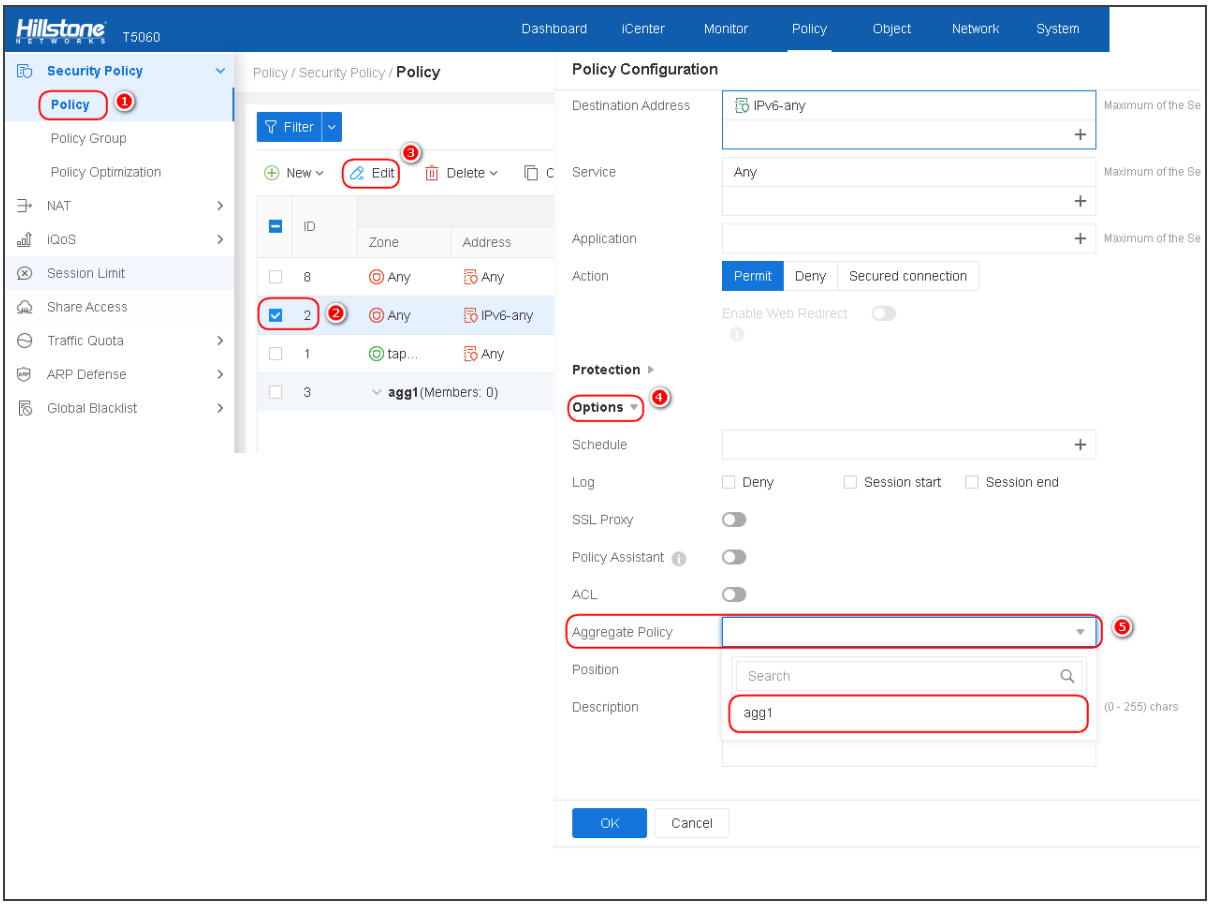
Option	Description
Name	Specifies the name of an aggregate policy. The range is 1 to 95 characters.
Position	The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name. In the **Position** drop-down list, you can select a position for the aggregate policy.
Description	Type descriptions into the **Description** box.
Audit Comment	After the "Configuration Audit" function is enabled, this option is required when creating or modifying an aggregate policy, and you must add policy audit comments to the text box. The range is 1 to 255 characters. For detailed operation of this function, please refer to Configuring Policy Audit Function. When the "Configuration Audit" function is not enabled, this option is optional and the range is 0 to 255 characters. For enabling/disabling the "Configuration Audit" function, please configure it in the **Option** page (**System > Device Management > Option**), refer to the Configuration Audit.

3. Click **OK** to save your settings.

Adding an Aggregate Policy Member

After creating an aggregate policy, the administrator can add a policy rule to the aggregate policy to be an aggregate policy member. There are two methods for adding an aggregate policy member.

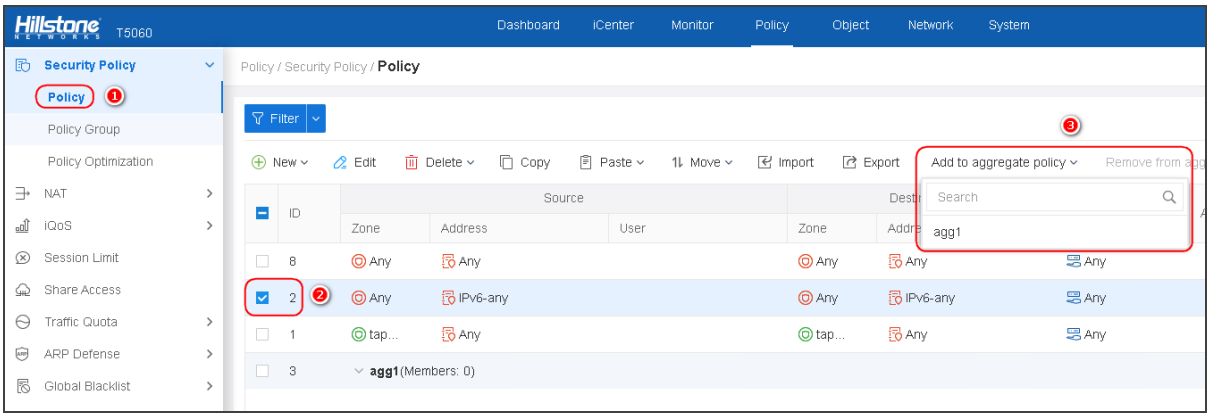
- Editing the policy configuration:



As shown above, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Select the policy rule that you want to add to an aggregate policy from the list.
3. Click **Edit** to open the **Policy Configuration** page.
4. Click **Options** to expand the relevant configuration items.
5. Click the **Aggregate Policy** drop-down menu, and select the aggregate policy to be added to the aggregate policy to which you want to add.
6. Click **OK**.

- Selecting a policy rule you want to add:

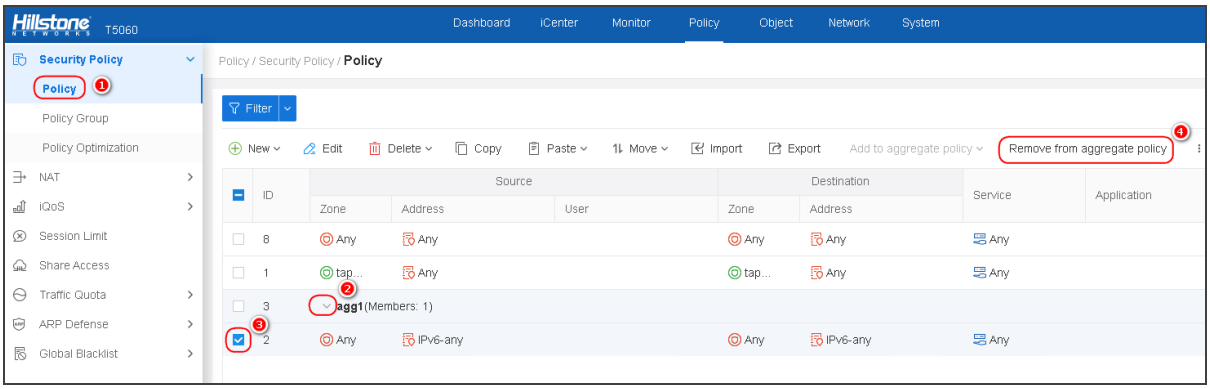


As shown above, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Select the policy rule that you want to add to an aggregate policy from the list. You can select multiple policy rules at a time
3. Click the **Add to aggregate policy** drop-down list, and select the aggregate policy to which you want to add.

Removing an Aggregate Policy Member

To remove a member from an aggregate policy, take the following steps:



1. Click **Policy** > **Security Policy** > **Policy**.
2. In the list, click the arrow before an aggregate policy to expand it
3. Select the aggregate policy member that you want to remove. You can select multiple policy rules at a time.
4. Click the **Move out from aggregate policy** button.



Notes:

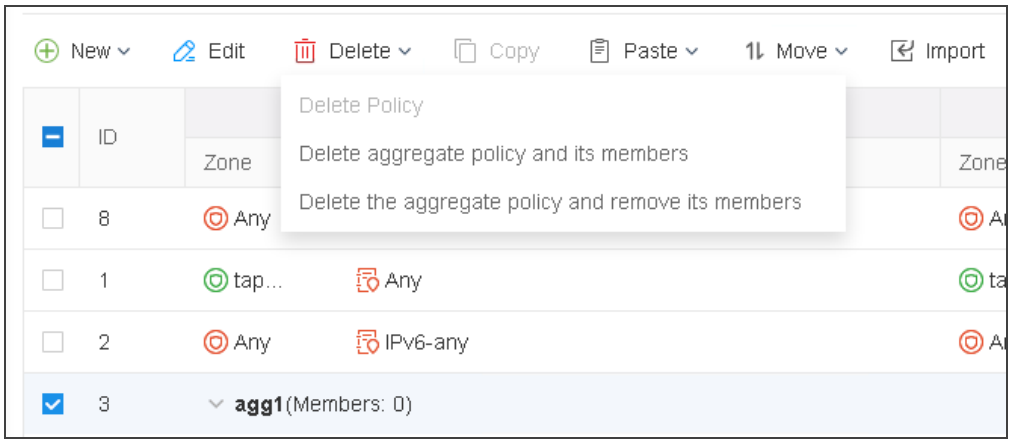
- If the member at the top position is removed from an aggregate policy, the removed member will be put before the aggregate policy.
- If a member at a non-top position is removed from an aggregate policy, the removed member will be put after the aggregate policy.
- If several aggregate policy members (including the member at the top position) in consecutive order are removed, they will be put before the policy all together.

Deleting an Aggregate Policy

To delete an aggregate policy, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Select the aggregate policy that you want to delete from the list.
3. Click **Delete**.

4. Select a deletion method from the drop-down list.



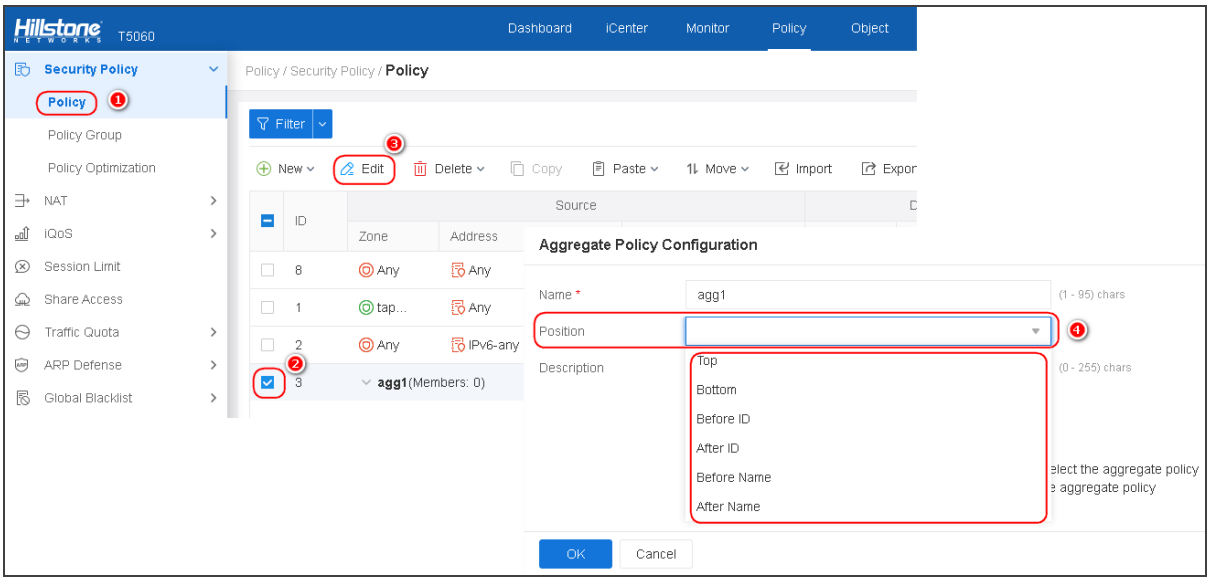
- Delete aggregate policy and members: When deleting an aggregate policy, the members in it will also be deleted.
- Delete aggregate policy, unbind members: When deleting an aggregate policy, all members in it will be removed.

5. Click **OK**.

Adjusting Position of an Aggregate Policy

The administrator can adjust the position of an aggregate policy by the following two methods. After the adjustment, the positions of all its members will be adjusted accordingly.

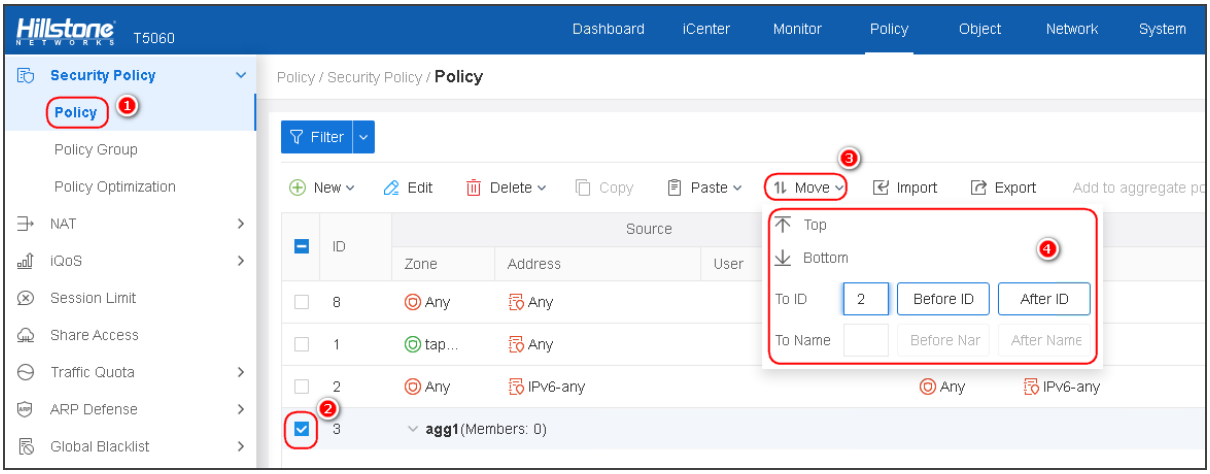
- Editing the aggregate policy configuration:



As shown above, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Select the aggregate policy whose position that you want to adjust from the list.
3. Click **Edit** to open the **Aggregate Policy Configuration**page.
4. Click the **Position** drop-down list, select a position for the aggregate policy.

- Adjust directly in the policy list:



As shown above, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Select the aggregate policy whose position that you want to adjust from the list.
3. Click **Move**.
4. In the pop-up menu, click **Top**, **Bottom** or type the rule ID /name , and click **Before ID** , **After ID** , **Before Name** or **After Name**. Then the rule will be moved before or after the specified ID or name.



Notes:

- The method for adjusting the position of an aggregate policy member is the same as the method for adjusting the position of an aggregate policy.
- The position adjustment for an aggregate policy member can only be performed in the aggregate policy to which it belongs.
- It is not supported to add a policy rule to or remove a policy rule from an aggregate policy by adjusting the position of the policy rule.

Enabling/Disabling an Aggregate Policy

By default, the configured aggregate policy will take effect immediately. By disabling an aggregate policy, the administrator can terminate its control over the traffic.

To enable/disable an aggregate policy, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy**.
2. Select the aggregate policy that you want to enable/disable from the list.
3. Click ⋮, and then select **Enable** or **Disable** to enable or disable the aggregate policy.

The disabled rule will not display in the list. Click ⋮, and then select **Show Disabled Policies** to show them.



Notes:

- After disabling an aggregate policy, its members will be disabled too.
- After enabling an aggregate policy, the original status (enabled/disabled) of its members will remain unchanged. For example, if the original status of an aggregate policy member is "disabled", the status will remain unchanged after the policy to which it belongs is enabled.

Configuring a Policy Group

You can organize some policy rules together to form a policy group, and configure the policy group directly.

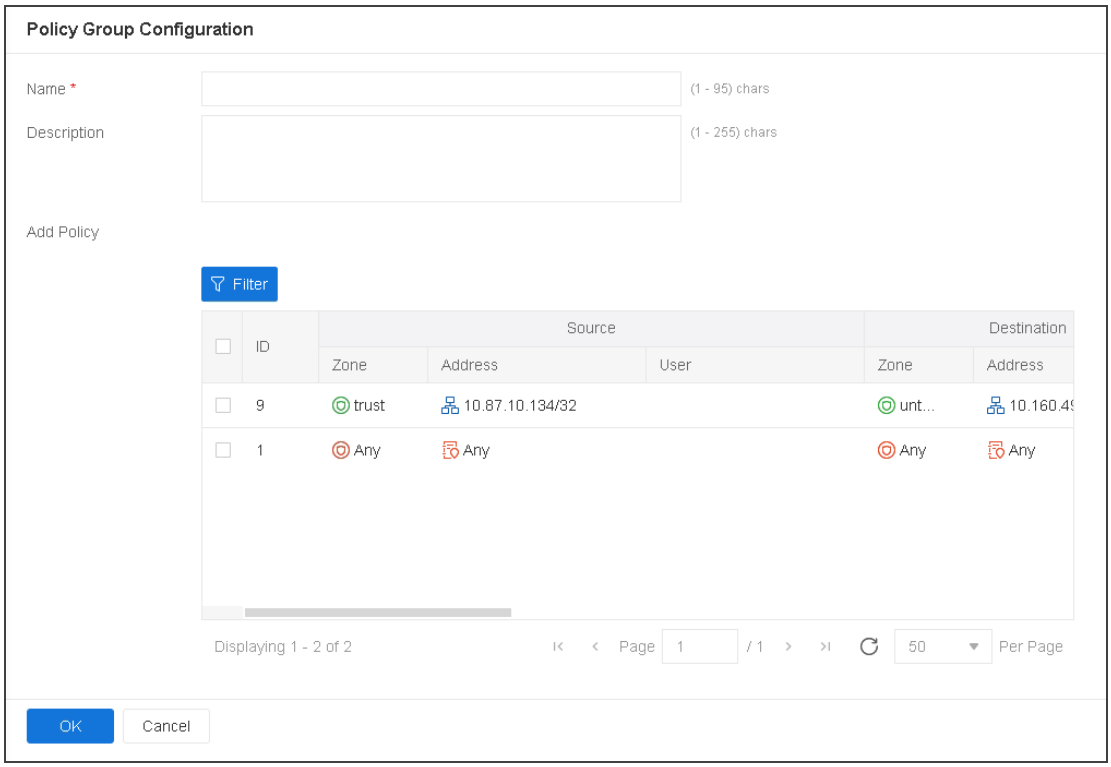
Configuring a security policy group include the following matters: creating a policy group, deleting a policy group, enable/disable a policy group, add/delete a policy rule member, edit a policy group and show disabled policy group.

Creating a Policy Group

To create a policy group, take the following steps:

1. Select **Policy > Security Policy > Policy Group** .

2. Click **New** to open the **Policy Group Configuration** page.



Configure the corresponding options.

Option	Description
Name	Specifies the name of the policy group. The length is 1 to 95 characters.
Description	Specifies the new description. You can enter at most 255 characters.
Add Policy	In the policy rules list, select the security policy rule that you want to add to the policy group.

3. Click **OK** to save your settings.

Deleting a Policy Group

To delete a policy group, take the following steps:

1. Select **Policy > Security Policy > Policy Group** .
2. Select the check box of the policy group that you want to delete, and click **Delete**.

Enabling/Disabling a Policy Group

By default the configured policy group will take effect immediately.

To enable/disable a policy group, take the following steps:

1. Select **Policy > Security Policy > Policy Group** .
2. Select the check box of the policy group that you want to enable or disable, and click the enable button under **Status** column. The enabled state is displayed as  , and the disabled state is displayed as  .

Adding/Deleting a Policy Rule Member

To add a policy rule member to the policy group, take the following steps:

1. Select **Policy > Security Policy > Policy Group** .
2. In the policy group list, click the "+" in front of the policy group item to expand the member list of the policy group.
3. Click **Add Members** button to open the **Policy Group-Add policy** page, which displays the list of policy rules that are not added to policy group.

4. Select the check box of the policy rules that you want to add to the policy group.
5. Click **OK** to save your settings.


Notes: A policy rule only can be added to a policy group.

To delete a policy rule member to the policy group, take the following steps:

1. Select **Policy > Security Policy** .
2. At the top-right corner of list, click **Policy Group** to enter the **Security Policy Group** page.
3. In the policy group list, click the "+" in front of the policy group item to expand the member list of the policy group.
4. Select the check box of the policy group that needs to be deleted, and click **Delete**.

Editing a Policy Group

To modify the name or description of policy group, take the following steps:

1. Select **Policy > Security Policy > Policy Group** .
2. Select the check box of the policy group that you want to edit, and click **Edit**.
3. Modify the name or description of policy group in the **Policy Group Configuration** page.

Showing Disabled Policy Group

To show disabled policy groups, take the following steps:

1. Select **Policy > Security Policy > Policy Group**.

2. Select the check box of **Show Disabled Policy Group**. The disabled policy group will be displayed in the policy group list, otherwise the policy group list will show only the enabled policy group.

Mini Policy

Mini policy is a kind of policy rule which only uses source / destination address, protocol, destination port, source / destination zone as traffic filtering conditions, and allows (Permit) or denies (Deny) as processing behavior. At the same time, system supports the configuration of a large number of mini policies, so it can meet more policy storage requirements.

The maximum number of mini policies supported by different device platforms is different, please refer to the actual device limit (Capacity).



Notes:

- Mini policy does not support adjusting priority.
- The matching priority of the policy is: mini policy> policy rule> default action, that is, system traffic will first match the mini policy, and then match the policy rule. When it is not matched with any configured mini policy or policy rule, system will process the traffic according to the specified default action.

  For the configuration of the default action, see Configuring Default Action.

Configuring a Mini Policy

The configuration of mini policy includes:

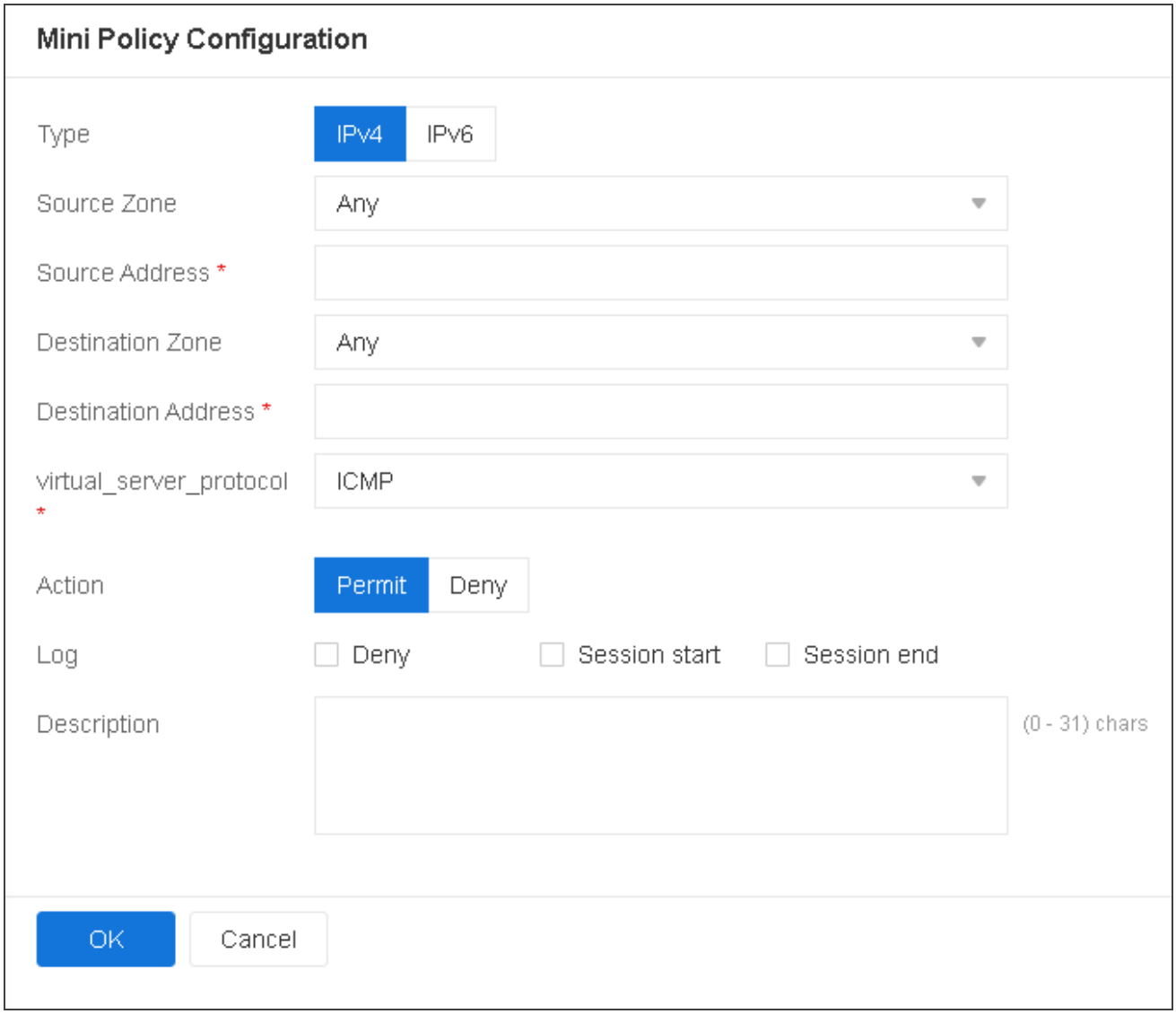
- Creating / Deleting a mini policy
- Editing a mini policy

- Viewing the mini policy information
- Viewing the mini policy hit information

Creating a Mini Policy

To create a mini policy, take the following steps:

1. Select **Policy > Security Policy > Mini Policy**.
2. Click **New** to open the **Mini Policy Configuration** page.



Configure the corresponding options.

Option	Description
Type	Specifies the IP address type, you can select **IPv4** or **IPv6**. This option can only be configured when the version supports IPv6; after selection, system only supports the configuration of IPv6 format IPv6/prefix length, IP address range or IP address entry.
Source Zone	Specifies the source zone of the mini policy. If not specified, the default value is any. Click the drop-down list, select the created zone, and click ⊕ to create a new zone. If not specified, the default is "Any".
Source Address (Required)	Specifies the source address of the mini policy. Enter the source address in the text box, which can be specified as an IPv4 address or an IPv6 address.
Destination Zone	Specifies the destination zone of the mini policy. If not specified, the default value is any. Click the drop-down list, select the created zone, and click ⊕ to create a new zone. If not specified, the default is "Any".
Destination Address (Required)	Specifies the destination address of the mini policy. Enter the source address in the text box, which can be specified as an IPv4 address or an IPv6 address.
Protocol Type (Required)	Select the protocol type from the drop-down list.
Destination Port	When the protocol type is specified as TCP or UDP, the destination port must be specified. The value range is 1-65535. For

Option	Description
	other protocol types, this option is not supported.
Action (Required)	Specifies the action of the mini policy, including: • Permit: Permits the traffic to pass through. • Deny: Denies the traffic.
Log	You can log policy rule matching in the system logs according to your needs, multiple options are available. • Deny: Record session rejection log information. • Session start: Record session establishment log information. • Session end: Record log information of session end.
Destination	Specifies the description of the mini policy. The length of *description* is 0 to 31 bytes.

3. Click **OK** to save your settings

Deleting a Mini Policy

To delete a mini policy, take the following steps:

1. Select **Policy > Security Policy > Mini Policy**.
2. Select the check box of the mini policy that you want to delete, and click **Delete**.

Editing a Mini Policy

To modify the configuration of mini policy, take the following steps:

1. Select **Policy > Security Policy > Mini Policy**.
2. Select the check box of the mini policy that you want to edit, and click **Edit**.
3. Modify the configuration of mini policy in the **Mini Policy Configuration** page

Notes: The type of mini policy cannot be modified.

Enabling/Disabling a Mini Policy

By default the configured mini policy will take effect immediately.

To enable/disable a mini policy group, take the following steps:

1. Select **Policy > Security Policy > Mini Policy** .
2. Select the check box of the mini policy that you want to enable or disable.
3. Click ⋮ icon , and then select **Enable** or **Disable** to enable or disable the rule.

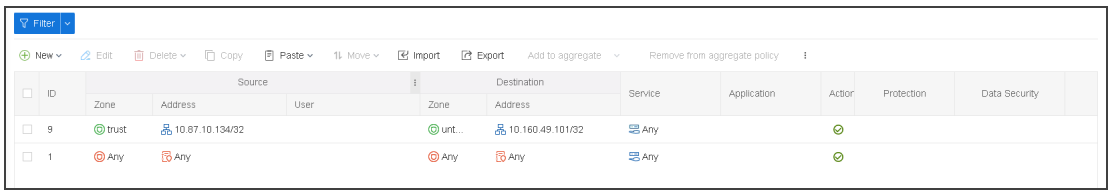
The disabled rule will not display in the list. Click ⋮ icon , and then select **Show Disabled Mini Policies** to show them.

Viewing and Searching Security Policy Rules/ Policy Groups/ Mini Policy

You can view and search the policy rules or policy groups in the policy/ policy group/ mini Policy list.

Viewing the Policy/ Policy Group/ Mini Policy

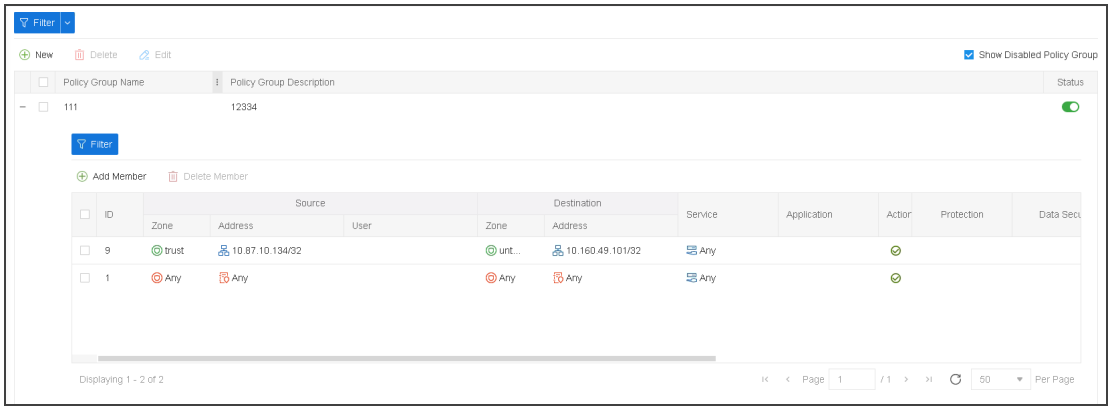
View the security policy rules in the policy rule list.



- Each column displays the corresponding configurations.
- Click  icon under the Session Detail column in the Policy list to open then the **Session Detail** page. You can view the current session status of the selected policy.
    - You can also click 

button to add filtering conditions and search out the filtered sessions.
    - The sessions whose timeout period is longer than or equal to 1 day are persistent sessions. You can select Long Session to view the status of persistent sessions. For more information, see Session Timeout.
- Hover over your mouse on the configuration in a certain column. Then based on the configuration type, the WebUI displays either icon or the detailed configurations.
    - You can view the detailed configurations directly.
    - You can click icon. Based on the configuration type, the WebUI displays **Add Filter** or **Details**.
        - Click **Details** to see the detailed configurations. Then, in the **Details** section, click **View** next to **Entry Details** to view the details about the address or service.
        - Click **Add Filter**, the filter condition of the configuration you are hovering over with your mouse appears on the top of the list, and then you can filter the policy according to the filter condition. For detailed information of filtering policy rules, see Searching Security Policy Rules/ Policy Groups.

View the policy groups in the policy group list.



- Each column displays the corresponding configurations.
- You can view the current policy group status in **Status** column. The enabled state is displayed as  , and the disabled state is displayed as  .

View the mini policy rules in the policy group list.



- Each column displays the corresponding configurations.
- The **ID** column shows the ID automatically assigned by the system for the mini policy. The ID must be unique in the entire system. The starting ID of the mini policy is 1000001, and the ID range varies according to different device platforms.

Searching Security Policy Rules/ Policy Groups/ Mini Policy

Use the Filter to search for the policy rules/ policy groups/ mini policy that match the filter conditions.

1. Click **Policy > Security Policy > Policy**, **Policy > Security Policy > Policy Group** or **Policy > Security Policy > Mini Policy**.

2. On the Policy/ Policy Group/ Mini Policy page, click **Filter** in the upper-left corner, select a filter condition from the drop-down menu, and enter a value. Filter conditions include Aggregate/ Authorization Policy or Not, Aggregate Policy, Reference Schedule, Schedule Status, Name, ID, Source Zone, Source Address, User, Destination Zone, Destination Address, Service, Application, VLAN ID, Action, and Description.
   When filtering policies by User, you can perform precise or fuzzy query to search policies that match the filter condition. Precise query is the default query method.

   - Fuzzy: Fuzzy query is performed by specifying the keyword of the user name / user group name/ role name. By fuzzy matching the specified keyword, a list of all policies that contain this keyword in their user name/ user group name/ role name will be returned.

     - Select **User** from the **Filter** drop-down list and select **Fuzzy**. Enter the keyword of the user name/ user group name/ role name in the text box. Click **Enter** to search for the policy rules that matches the filter conditions.

   - Precise: Precise query is performed by specifying a precise user name/ user group name. By precise matching the specified user name/ user group name, a list of all policies that have the same user name/ user group name will be returned. If a policy's user group contains the specified user name/ user group name, this policy will also be listed in the search results.

     - Select **User** from the **Filter** drop-down list and select **Precise**. From the drop-down list, select the AAA server where user/ user group resides. Then, click **Select User** or **Select User Group** from the drop-down list and select existing user name/ user group name. Click **Enter** to search for the policy rules that

matches the filter conditions. You can also select **Input User** or **Input User-group** and specify the user name/ user group name in the text box.

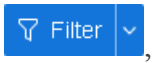
Notes:

- Policy group and mini policy do not support the **User** filter condition.
- **Fuzzy** and **Precise** are mutually exclusive and cannot be selected at the same time.
- When **Precise** is specified, you need to specify the AAA server. In this case, the AAA server can only be Local server, AD server, and LDAP server. If AD server or LDAP server is specified, and **Input User** or **Input Usergroup** is specified, only policies that have the same user name/ user group name will be searched. If a policy's user group contains the specified user name/ user group name, this policy cannot be searched.

3. Click **Filter** to add a new filter condition. Then select a filter condition from the drop-down menu and enter a value.
4. Press **Enter** to search for the policy rules that matches the filter conditions.
5. Repeat the above two steps to add more filter conditions. The relationship between each filter condition is **AND**.
6. To delete a filter condition, hover your mouse on that condition and then click ✕Remove All icon. To close the filter, click ✕ icon on the right side of the row.



Save the filter conditions.

1. After adding the filter conditions, click  in , in the drop-down menu, click **Save Filters**.
2. Specifies the name of the filter condition to save, the maximum length of name is 32 characters, and the name supports only Chinese and English characters and underscores.
3. Click the **Save** button on the right side of the text box.
4. To use the saved filter condition, double click the name of the saved filter condition.
5. To delete the saved filter condition, click  on the right side of the filter condition.



Notes:

- You can add up to 20 filter conditions as needed.
- After the device has been upgraded, the saved filter condition will be cleared.

Policy Optimization

If you want to clear up the rules which haven't been used for a long time, it is hard to determine which policy rules need to be deleted when there are a large number of policy rules on the device. The system supports to operate the Policy Hit Analysis, operate the Rule Redundancy Check, and configure the Policy Assistant.

Policy Hit Analysis

Policy Hit Analysis is a process to check the policy rule hit counts, that is, when traffic matches a certain policy rule, the hit count will increase by 1 automatically. With the statistics of the first hit time, the last hit time, and the days since last hit, you can identify the policy rule that need to be cleared. You can view the specified policy rules by setting up filters.

To check the hit counts, take the following steps:

1. Select **Policy > Security Policy > Policy Optimization**, and select the **Policy Hit Analysis** tab.
2. Select filter conditions from the **Filter** drop-down list, and configure filter conditions as needed.

   Configure the options as follows.

Option	Description
Policy ID	Displays hit statistics of the policy rule whose ID is the specified ID
Hit count<	Displays the policy rules whose hit count is less than a specified value.
Upstream Packets<	Displays the policy rules where the number of upstream packets of the system traffic hitting these policy rules is less than a specified value.
Downstream Packets<	Displays the policy rules where the number of downstream packets of the system traffic hitting these policy rules is less than a specified value.
Upstream Bytes<	Displays the policy rules where the number of upstream bytes of the system traffic hitting these policy rules is less than a specified value.
Downstream Bytes<	Displays the policy rules where the number of downstream bytes of the system traffic hitting these policy rules is less than a specified value.
Days Since First Hit>	Specify the day after the first hit. Then the policy rules which were hit before the specified day will be displayed.

Option	Description
Days Since Last Hit>	Specify the day after the last hit. Then the policies rules before the specified day will be displayed.
Days Since Policy Created>	Specify the day after the policy is created. Then the policy rules before the specified day will be displayed.

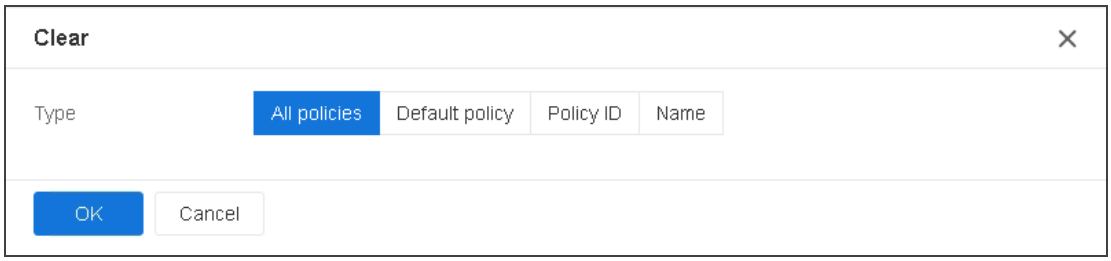
3. Click the **Export** button, and the analysis of the filtered policy rules will be exported in the format of CSV.
4. Click **Enter** or any blank space on the page to view the latest result of Policy Optimization.
5. Click + icon in front of policy ID to view the details of the policy rule.
6. Click 

icon on the right side of to save the selected filters. Click **Save Filters**, type the name of the filters and click Save. After saved, the combined filters can be selected directly in the drop-down list.
7. To delete a filter condition, hover your mouse on that condition and then click × icon. To delete all filter conditions, click ×Remove All icon on the right side of the row.

To clear a policy hit count, take the following steps:

1. Select **Policy > Security Policy > Policy Optimization**, and select the **Policy Hit Analysis** tab.

2. Click **Clear** to open the **Clear** page.



Configure the following options.

Option	Description
All policies	Clears the hit counts of all policy rules.
Default policy	Clears the hit counts of the default action policy rules.
Policy ID	Clears the hit counts of a specified ID policy rule.
Name	Clears the hit counts of a specified name policy rule.

3. Click **OK**.

You can also perform other operations:

- Click icon to delete the policy rule.
- Click icon to disable the policy rule.
- Click icon to clear the policy hit count.

Rule Redundancy Check

To ensure the validity of policy rules, the system can perform redundancy check on policy rules to check whether redundant or conflict policies exist. The system considers the source zone, source address, source device, destination zone, destination address, destination device, service, application, and VLAN ID of policy rules as redundancy check items. It sequentially compares high-priority policies with low-priority policies for analysis and lists the analysis results in the redundancy check list for further processing, which helps you streamline policies.

Redundancy check supports four types of checks: completely redundancy, partly redundancy, completely conflict, and partly conflict.

- Completely redundancy: The redundancy check items of Policy A are completely covered by Policy B. When Policy A has lower priority than Policy B and the actions are the same, Policy A will be checked as completely redundant.
- Partly redundancy: Each redundancy check item of two policy rules has partial overlap, and the actions are the same. The policy rule with a lower priority will be checked as partially redundant.
- Completely conflict: The redundancy check items of Policy A are completely covered by Policy B. When Policy A has lower priority than Policy B and the actions conflict, Policy A will be checked as completely conflict.
- Partly conflict: Each redundancy check item of two policy rules has partial overlap, and the actions conflict. The policy rule with a lower priority will be checked as partly conflict.



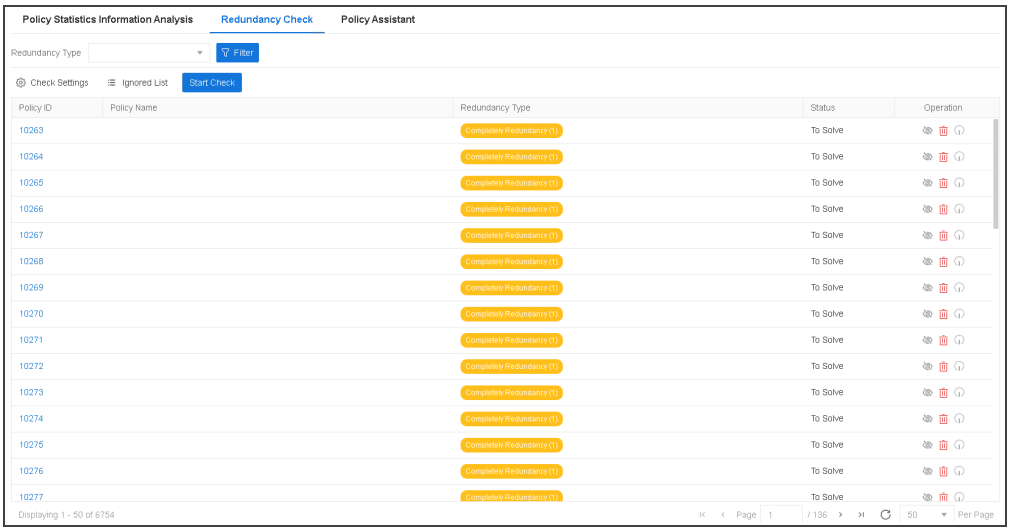
Notes: The Redundancy Check function takes effect only on policy rules whose action is "Permit" or "Deny".

Performing Redundancy Check on Policy Rules

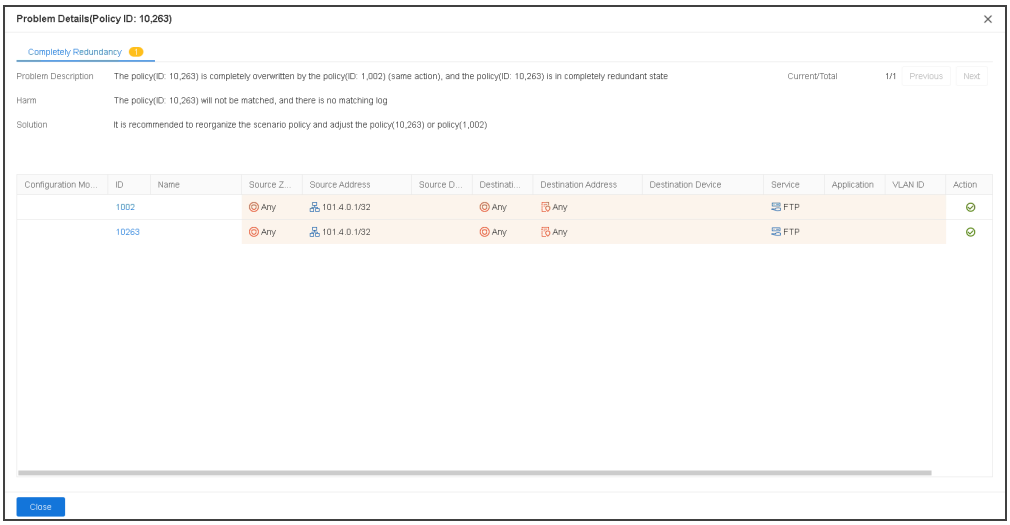
To perform redundancy check on policy rules, take the following steps:

1. Select **Policy > Security Policy > Policy Optimization**, and select the **Redundancy Check** tab.
2. Click **Check Settings** to specify the issue types of redundancy check. The system supports to check multiple issue types at the same time. When you check multiple issue types at the same time, the check time increases. If not specified, "Completely Redundancy" and "Completely Conflict" are selected.

3. Click **Start Check**. This process may take some time. Once completed, policy rules with identified issues will be displayed in the redundancy check list. During the check process, a check status bar will appear in the lower-left of the page. It is recommended not to configure or edit policy rules while the process is ongoing. You can click ✕ to manually stop the check process as required. After you click this button, the system will prompt a confirmation dialog, click **OK** to stop the check.



4. In the redundancy check list, click the label in the **Redundancy Type** column of the specified policy rule to open the **Problem Details** page and view the problem description, hazard, and solution of the specified policy rule.



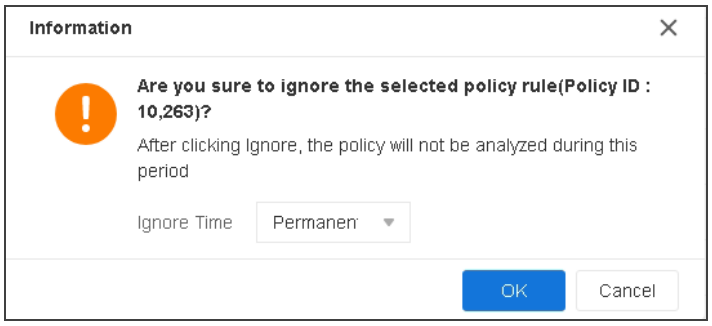
- Configuration entries that are problematic for a policy rule are highlighted in orange in the list on the **Problem Details** page.
- You can edit a policy rule by clicking the policy rule ID or policy name. For more information, see Configuring a Policy Rule.
- There are up to 100 policy rules for each type of issue, and you can switch between them by clicking **Previous** and **Next** in the upper-right of the page.

Configuring Ignored Time of Redundant Policy Rules

For the redundant policy rules checked by the system, you can ignore the redundant policy rules as required and specify the ignore time for them. Ignored redundant policy rules can be viewed or un-ignored in the ignored list, and the system will no longer check the redundancy of the policy rule during the ignore time.

To configure the ignore time of redundant policy rules, take the following steps:

1. Select **Policy > Security Policy > Policy Optimization**, and select the **Redundancy Check** tab.
2. In the redundancy check list, click in the **Operation** column. Then, in the dialog box that appears, select a ignored time, including permanent, 7 days, 15 days, and user-defined. The user-defined time range is 1 to 3650 days.



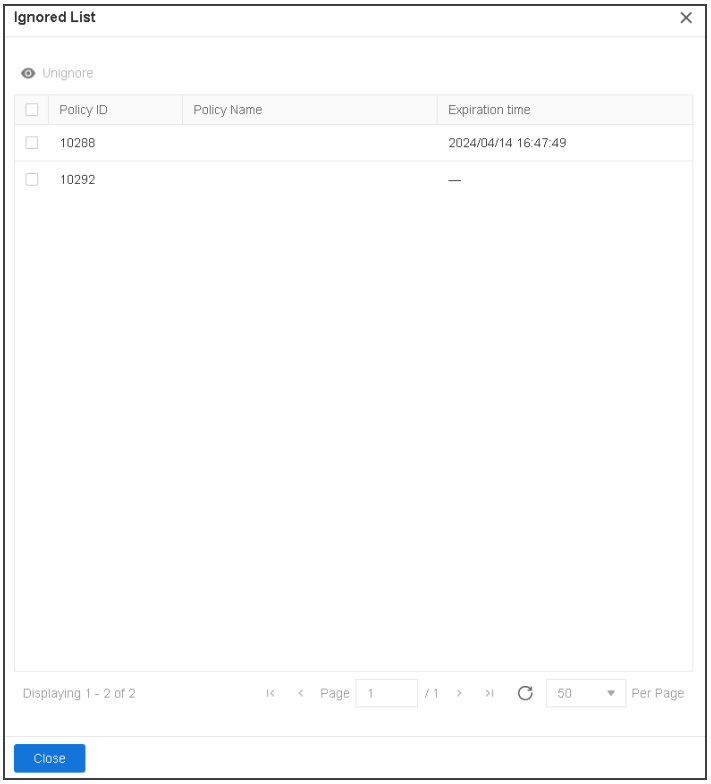
3. Click **OK**.

Managing the Ignored List

The ignored list displays the redundant policy rules that have been ignored. You can view the information of the ignored policy rules in this list and can also unignore them as needed.

To manage the ignored list, take the following steps:

1. Select **Policy > Security Policy > Policy Optimization**, and select the **Redundancy Check** tab.
2. Click **Ignored List**. The Ignored List panel displays the policy ID, name, and expiration time of ignored redundant policy rules.



   Note: "—" in the **Expiration time** column indicates that the ignored time is permanent.

3. Select one or more ignored policy rule and click **Unignore** to unignore them.
4. Click **Close**.

In the redundancy check list, you can also perform the following operations:

- Click the policy rule ID or policy name to edit the policy rule. For more information, see Configuring a Policy Rule.
- Click in the **Operation** column to delete the policy rule.
- Click in the **Operation** column to disable the policy rule.

Configuring the Policy Assistant

The policy assistant can help users generate targeted policies more quickly and accurately. With the function, system can analyze the traffic of a specified policy ID, optimize the traffic via setting replacement conditions and aggregation conditions, generate address books and service books on the basis of the traffic, and then generate the target policies.

Click **Policy** > **Security Policy** > **Policy Optimization**, and select the **Policy Assistant** tab. In the **Policy Assistant** tab, generate target policies as the wizard:

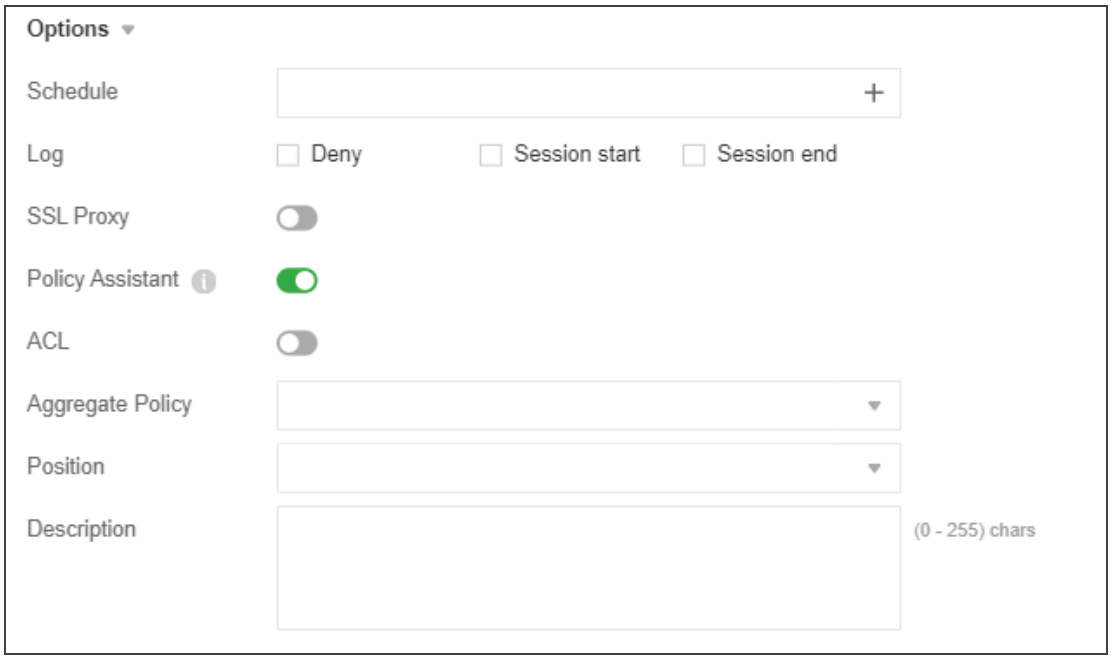
Display Traffic->Replace ->Aggregate -> Generate Address book ->Generate Service book ->Generate Policy

Enabling the Policy Assistant

Before configuring policy assistant related function, please enable the function first.

1. Select **Policy** > **Security Policy** > **Policy**.
2. Create a rule or select an existing rule which needs to enable the policy assistant function and click **Edit** to open the **Policy Configuration** page.

3. Expand **Options**, and click the **Policy Assistant** button to enable the function.



Notes: For the root VSYS, at most 4 policies are allowed to enable the policy assistant function, while for the non-root VSYS, only 1 policy can enable the function.

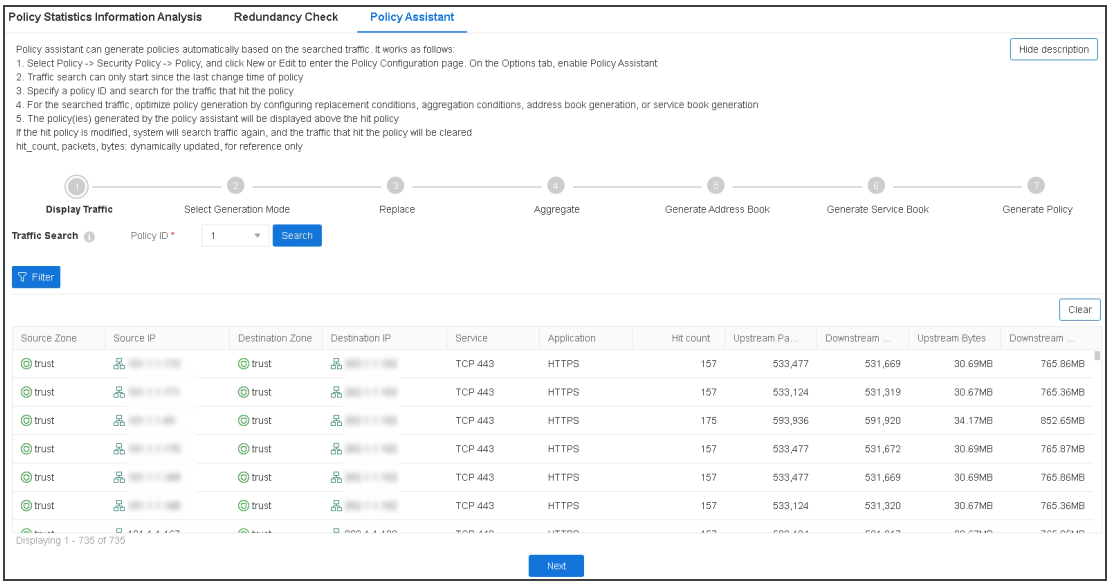
Displaying Traffic

On the Display Traffic page, the source zone, source IP, destination zone, destination IP, service, number of hits, the number of upstream packets, the number of downstream packets, the number of upstream bytes, and the number of downstream bytes of traffic hit the selected policy ID will be displayed.

To display the traffic data, take the following steps:

1. Click **Policy** > **Security Policy** > **Policy Optimization**, and select the **Policy Assistant** tab.

2. Click **Display Traffic** on the configuration wizard.



Configure the options as follows:

Option	Description
Traffic Search	Select the ID of policy which has enabled the policy assistant function from the **Policy ID** drop-down list, click **Search Traffic** and the traffic hit the policy will be displayed in the following list. **Note:** • At most 1,000 traffic data can be displayed in the list. If the traffic data exceeds 1,000, the oldest traffic data will be covered. • If the selected policy is edited, or the policy assistant function is disabled or the device is rebooted, the traffic data will be cleared.

Option	Description
Filter	Click Filter to specify filter conditions. The logical operator among filter conditions is AND. Filter conditions are described as follows. • Source IP: Displays the traffic data of the specified source IP address. The source IP address can be in the IP/subnet mask or IP range format. • Destination IP: Displays the traffic data of the specified destination IP address. The destination IP address can be in the IP/subnet mask or IP range format. • Protocol: Displays the traffic data of the specified protocol. • Hit count: Displays the traffic data whose hit count is less than or equal to (<=) or greater than or equal to (>=) a specified value. • Upstream Packets: Displays the traffic data whose number of upstream packets is less than or equal to (<=) or greater than or equal to (>=) a specified value. • Downstream Packets: Displays the traffic data whose number of downstream packets is less than or equal to (<=) or greater than or equal to (>=) a specified

Option	Description
	value. • Upstream Bytes: Displays the traffic data whose number of upstream bytes is less than or equal to (<=) or greater than or equal to (>=) a specified value. • Downstream Bytes: Displays the traffic data whose number of downstream bytes is less than or equal to (<=) or greater than or equal to (>=) a specified value.
Traffic Filtering	Edit filtering conditions, and the filtered traffic data will be displayed in the list.
Hide description/Show description	Click the **Hide description** or **Show description** button in the upper right corner to view/hide the step-by-step instructions of policy assistant.
Clear	Click the **Clear** button to delete the searched traffic data in the list. **Note**: Make sure the searched traffic has been analyzed before clearing.

3. Click **Next** to enter into the next configurations.

Replacing Policy

You can set the condition of source IP, destination IP or service. When the items of policies meet the condition, the items will be replaced with the condition.

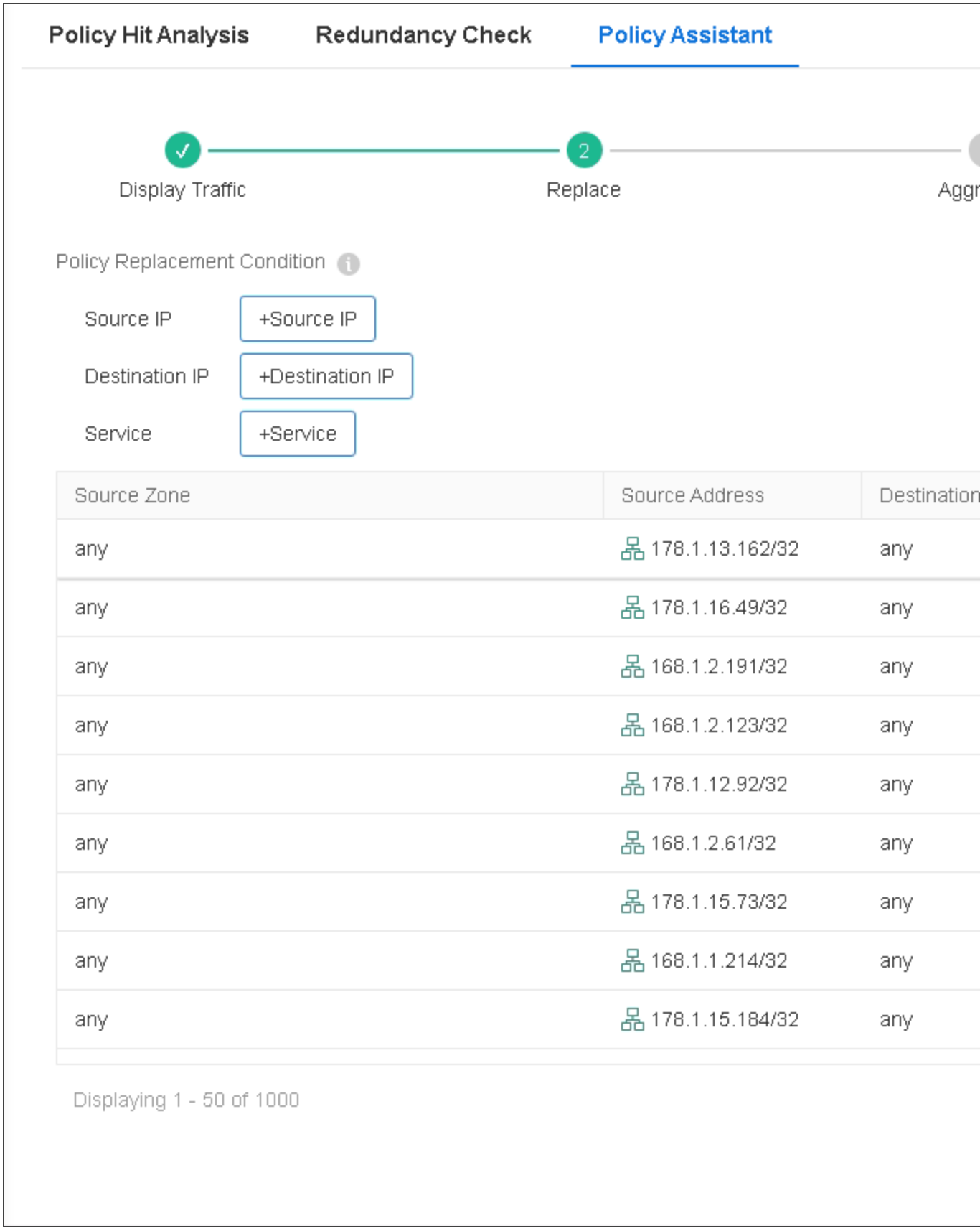
Application Scenario Example

For example, when the admin get some traffic data originating form 172.16.1.10. After the analysis of the traffic data, the source IP is judged as normal. What's more, all IP address of 172.16.1.0/24 is judged as normal too. To enlarge the source IP range to 172.16.1.0/24, the admin can set the 172.16.1.0/24 as the replacement condition on the Replace Policy page, then the source IP of the searched traffic which is within the IP range will be changed to 172.16.1.0/24.

Configuring Replacement Conditions

To configure replacement conditions for the policy items, take the following steps:

1. Click **Replace Policy** on the configuration wizard.


Policy Hit Analysis
Redundancy Check
Policy Assistant
Display Traffic
2
Replace
Policy Replacement Condition
Source IP
+Source IP
Destination IP
+Destination IP
Service
+Service
Source Zone
Source Address
Destination
any
178.1.13.162/32
any
any
178.1.16.49/32
any
any
168.1.2.191/32
any
any
168.1.2.123/32
any
any
178.1.12.92/32
any
any
168.1.2.61/32
any
any
178.1.15.73/32
any
any
168.1.1.214/32
any
any
178.1.15.184/32
any
Displaying 1 - 50 of 1000

Configure the options as follows:

Option	Description
Source IP	Specify the replacement condition of source IP. At most 3 conditions can be set for the source IP. 1. Click the +Source IP button. 2. Select IP/Netmask or IP Range from the drop down list and set the replacement conditions as needed.
Destination IP	Specify the replacement condition of destination IP. At most 3 conditions can be set for the destination IP. 1. Click the +Destination IP button. 2. Select IP/Netmask or IP Range from the drop down list and set the replacement conditions as needed.
Service	Specify the replacement condition of service. At most 3 conditions can be set for the service. 1. Click the +Service button. 2. Specify the protocol from the drop-down list and set the port range as needed.

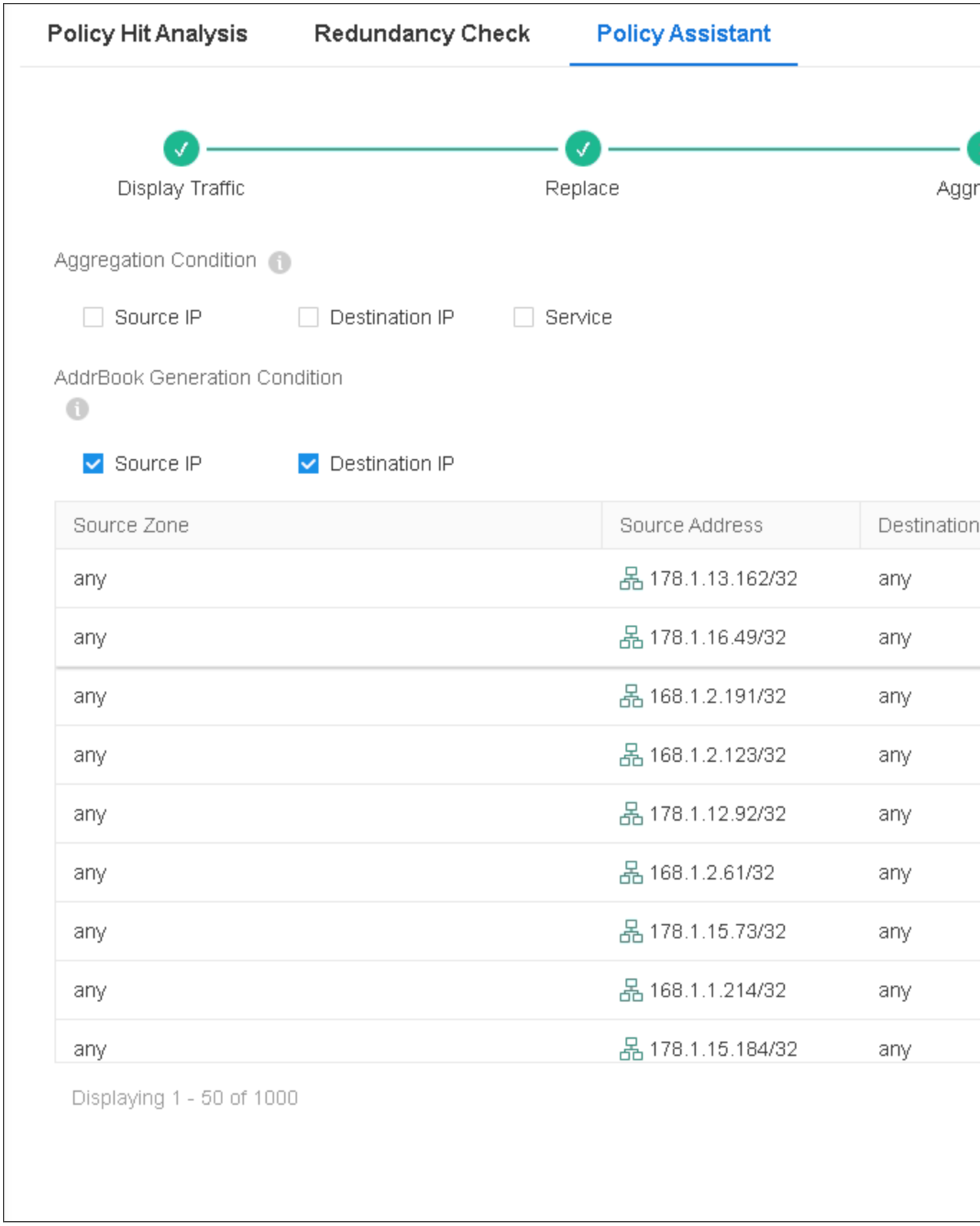
2. Click **Next** to enter into the next configurations.

Aggregating Policy

You can aggregate the policy items of the same source IP, destination IP and service, so as to reduce the redundant policies.

To aggregate policies, take the following steps:

1. Click **Aggregate Policy** on the configuration wizard.


Policy Hit Analysis
Redundancy Check
Policy Assistant
Display Traffic
Replace
Aggr
Aggregation Condition
Source IP
Destination IP
Service
AddrBook Generation Condition
Source IP
Destination IP
Source Zone
Source Address
Destination
any
178.1.13.162/32
any
any
178.1.16.49/32
any
any
168.1.2.191/32
any
any
168.1.2.123/32
any
any
178.1.12.92/32
any
any
168.1.2.61/32
any
any
178.1.15.73/32
any
any
168.1.1.214/32
any
any
178.1.15.184/32
any
Displaying 1 - 50 of 1000

2. Select the Aggregation conditions as Source IP, Destination IP , Service or Application, and the policy items in the list will be aggregated as the selected condition.

3. Select the Address Book Generation conditions as Source IP or Destination IP to enable the Address Book Generation function. In doing so, the corresponding address book entries will be listed in the "Generating Address book" procedure according to the generation conditions. By default, all the Address Book Generation conditions are selected. If no condition is selected, then the Address Book Generation function will be disabled, the "Generate Address Book" procedure will be removed from the configuration wizard, and the system generates policies based on IP address, not on address book.

4. Click **Next** to enter into the next configurations.

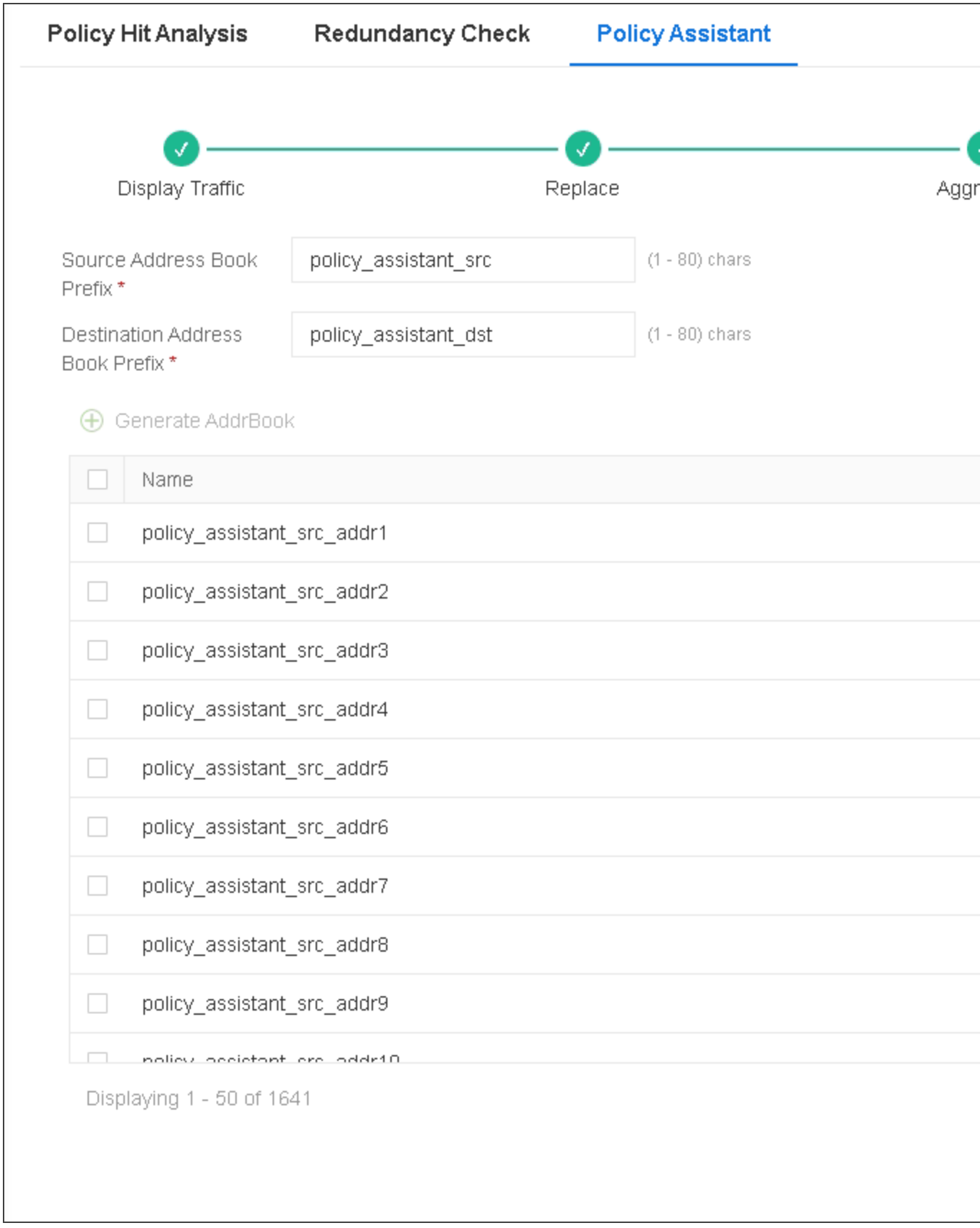
Generating Address book

The searched traffic data can display the Source IP and the Destination IP. After the procedures of replacing and aggregating, if the user select the Address Book Generation conditions in the **Aggregate** procedure and therefore generable address book entries are displayed in the **Generate Address book** page. According to your demands, you can select desirable entries to be generated as address books and then added into the system address books.

If you does not want to generate address books, then you can directly click **Next** to enter the next configurations.

To generate address book, take the following steps:

1. Click **Generate Address book** on the configuration wizard. The **Generate Address Book** page displays items of all address books, including the type, member and status.


Policy Hit Analysis
Redundancy Check
Policy Assistant
Display Traffic
Replace
Aggr
Source Address Book Prefix *
policy_assistant_src
(1 - 80) chars
Destination Address Book Prefix *
policy_assistant_dst
(1 - 80) chars
Generate AddrBook
Name
policy_assistant_src_addr1
policy_assistant_src_addr2
policy_assistant_src_addr3
policy_assistant_src_addr4
policy_assistant_src_addr5
policy_assistant_src_addr6
policy_assistant_src_addr7
policy_assistant_src_addr8
policy_assistant_src_addr9
Displaying 1 - 50 of 1641

2. Specify the prefix for the source address book in the list. The range is 1 -80 characters. The default prefix is "policy_assistant_src". When the prefix is specified, the name of address book in the list will be changed to "the specified prefix_addr+serial number".

3. Specify the prefix for the destination address book in the list. The range is 1 -80 characters. The default prefix is "policy_assistant_dst". When the prefix is specified, the name of address book in the list will be changed to "the specified prefix_addr+serial number".

4. Select the check box before the desirable address book entry and click **Generate Address book** button, the corresponding address book will be generated (which can be seen in **Object> Address book**). After successfully generating address books, the **Status** column will indicate **Generated**; if unsuccessfully, the Status column will indicate the failure reason.

5. Click **Next** to enter into the next configurations.

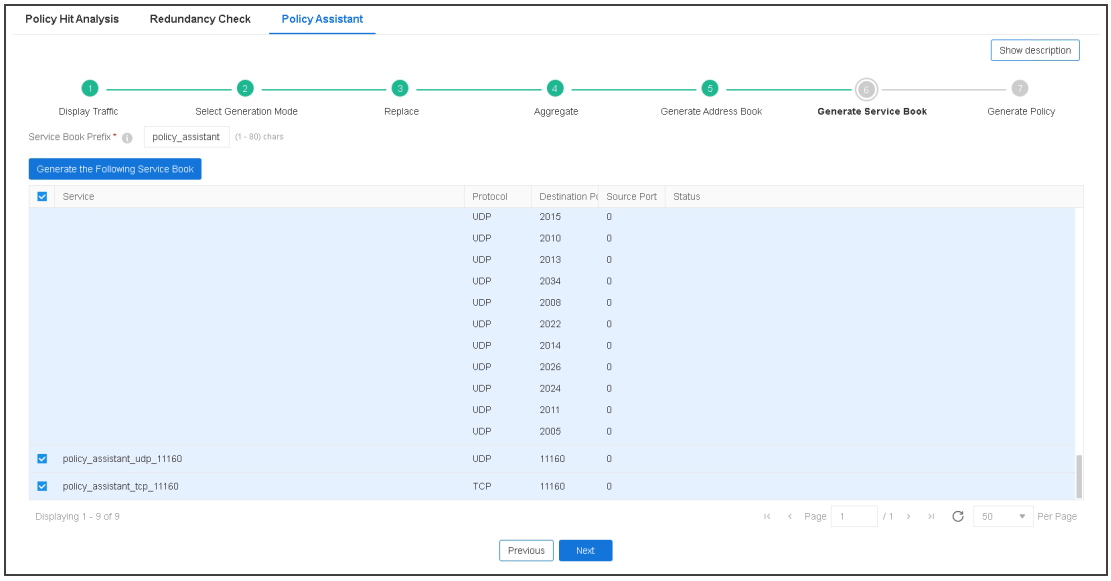
Generating Service Book

The searched traffic data can display the protocol and port, and you can generate corresponding service books based on the protocol and service. After replacing, aggregating, address book generation, generable service book entries are displayed in the **Generate Service book** page. According to your demands, you can select desirable entries to be generated as service books and then added into the system service books.

If you does not want to generate service books, then you can directly click **Next** to enter the next configurations.

To generate service, take the following steps:

1. Click **Generate Service Book** on the configuration wizard. The **Generate Service Book** page displays items of all service books, including the protocol, destination/source port and status.



2. Specify the prefix for the service book in the list. The range is 1 -95 characters. The default prefix is "policy_assistant". When the prefix is specified, the name of service book in the list will be changed to "the specified prefix + protocol configurations".

3. Select the check box before the desirable service book entry, click **Generate Service**, and the corresponding service book will be generated (which can be seen in **Object** > **Service Book** > **Service**). After successfully generating address books, the **Status** column will indicate **Generated**; if unsuccessfully, the Status column will indicate the failure reason.

4. Click **Next** to enter into the next configurations.

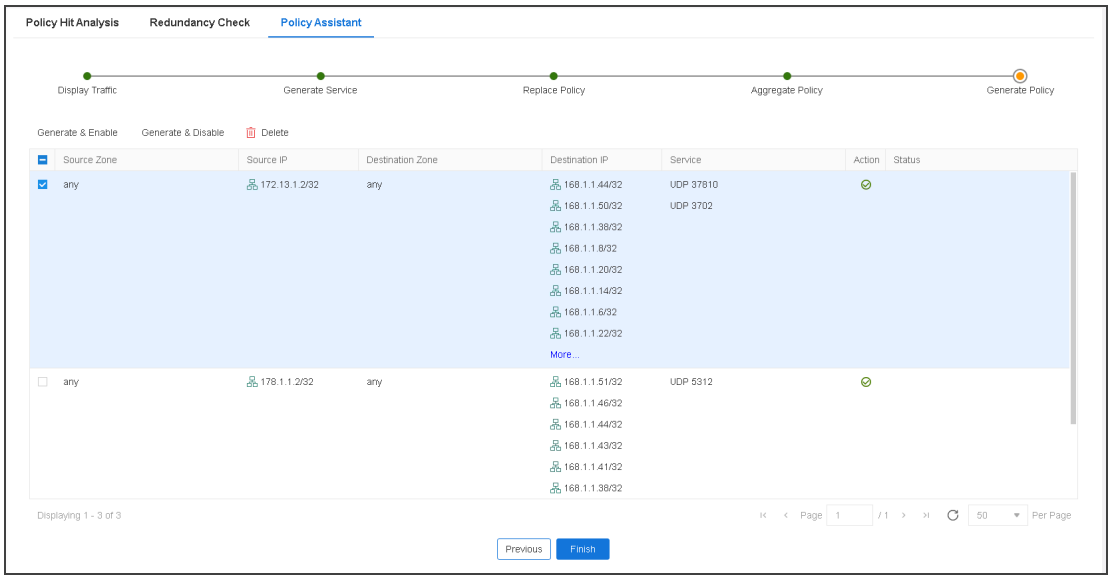
Generating Policy

The **Generate Policy** page displays all policy items after the configurations in **Replace**, **Aggregate**, **Generate Address Book** and **Generate Service Book** page. You can select policy items as needed to generate policy and the selected policy will be display on the **Security Policy** > **Policy** page.

Note: For the generated security policies, the source IP, destination IP, service and application are determined by the selected aggregation conditions, while the source zone, destination zone and action keep the same with the original policy items.

To generate policies, take the following steps:

1. Click **Generate Policy** on the configuration wizard.



Configure the options as follows:

Option	Description
Generate & Enable	Select the check box before the policy items as needed, click **Generate & Enable**, and the policies will take effect after generation. The generated policies will be displayed on the Policy page and on the above of the original policies.
Generate & Disable	Select the check box before the policy items as needed, click **Generate & Disable**, and the policies will not take effect after generation. The generated policies will be displayed on the Policy page and on the above of the original policies.
Delete	Select the check box before the policy items as needed, click **Delete**, and the policies will be deleted.

2. Click **Finish** to finish the configurations of policy assistant.

User Online Notification

The system provides the policy-based user online notification function. The user online notification function integrates WebAuth function and Web redirect function.

After configuring the user online notification function, system redirects your HTTP request to a new notification page when you visit the Internet for the first time. In the process, a prompt page (see the picture below) will be shown first, and after you click **continue** on this page, system will redirect your request to the specified notification page. If you want to visit your original URL, you need to type the URL address into the Web browser.



Before you enable the user online notification function, you must configure the WebAuth function. For more information about configuring WebAuth function, view "Web Authentication" on Page 470.

Configuring User Online Notification

To configure the user online notification function, take the following steps:

1. Select **Policy > Security Policy**.
2. Select the security policy rule with which you want to enable the user online notification function. Generally, it is recommended to select the security policy rule which is under the WebAuth policy rule and whose action is permit to transmit the HTTP traffic.
3. Click **Edit**.
4. In the Policy Configuration page, click the **Enable Web Redirect** button and type the notification URL into the **Notification page URL** box.
5. Click **OK** to save the settings.

Configuring the Parameters of User Online Notification

The parameters are:

- Idle time: The time that an online user stays online without traffic transmitting. If the idle time is exceeded, the HTTP request will be redirected to the user online notification page again.
- Background picture: You can change the background picture on the prompt page.

To configure the parameters, take the following steps:

1. Select **Policy > Security Policy**.
2. Select the security policy rule with the user online notification function enabled.
3. Click ⋮ and select **Web Redirect Configuration**.
4. Type the idle time value into the **Idle time** box. The default value is 30 minutes. The range is 0 to 1440 minutes.

5. Change the background picture of the prompt page. Click **Browse** to choose the picture you want, and then click **Upload**. The uploaded picture must be zipped and named as logo.jpg, with the suggested size of 120px*40px.

Viewing Online Users

After configuring the user online notification function, you can get the information of online users from the Online Notification Users dialog box.

1. Select **Policy > Security Policy**.
2. Click ⋮ and select **Web Redirect IP List**.
3. In the Web Redirect IP List page, view the following information.

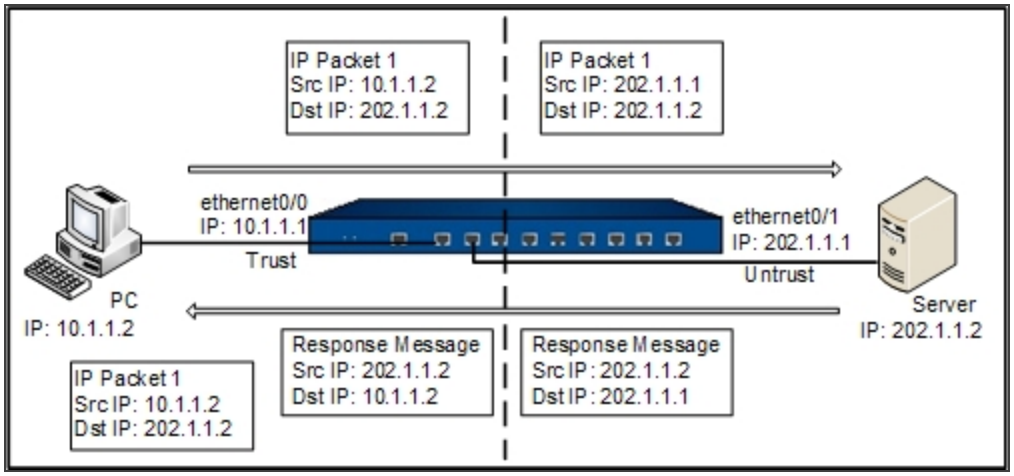
Option	Description
IP address	The IP address of the online user.
Sessions	Session number of the online user.
Interface	The source interface of the online user.
Lifetime (s)	The period of time during which the user is staying online.
Expiration (s)	The idle time of the user.

NAT

NAT, Network Address Translation, translates the IP address within an IP packet header to another IP address. When the IP packets pass through the devices or routers, the devices or routers will translate the source IP address and/or the destination IP address in the IP packets. In practice, NAT is mostly used to allow the private network to access the public network, vice versa.

Basic Translation Process of NAT

When a device is implementing the NAT function, it lies between the public network and the private network. The following diagram illustrates the basic translation process of NAT.



As shown above, the device lies between the private network and the public network. When the internal PC at 10.1.1.2 sends an IP packet (IP packet 1) to the external server at 202.1.1.2 through the device, the device checks the packet header. Finding that the IP packet is destined to the public network, the device translates the source IP address 10.1.1.2 of packet 1 to the public IP address 202.1.1.1 which can get routed on the Internet, and then forwards the packet to the external server. At the same time, the device also records the mapping between the two addresses in its NAT table. When the response packet of IP packet 1 reaches the device, the device checks the packet header again and finds the mapping records in its NAT table, and replaces the destination address with the private address 10.1.1.2. In this process, the device is transparent to the PC and the Server. To the external server, it considers that the IP address of the internal PC is

202.1.1.1 and knows nothing about the private address 10.1.1.2. Therefore, NAT hides the private network of enterprises.

Implementing NAT

The devices translate the IP address and port number of the internal network host to the external network address and port number, and vice versa. This is the translation between the "private IP address + port number" and "public IP address + port number".

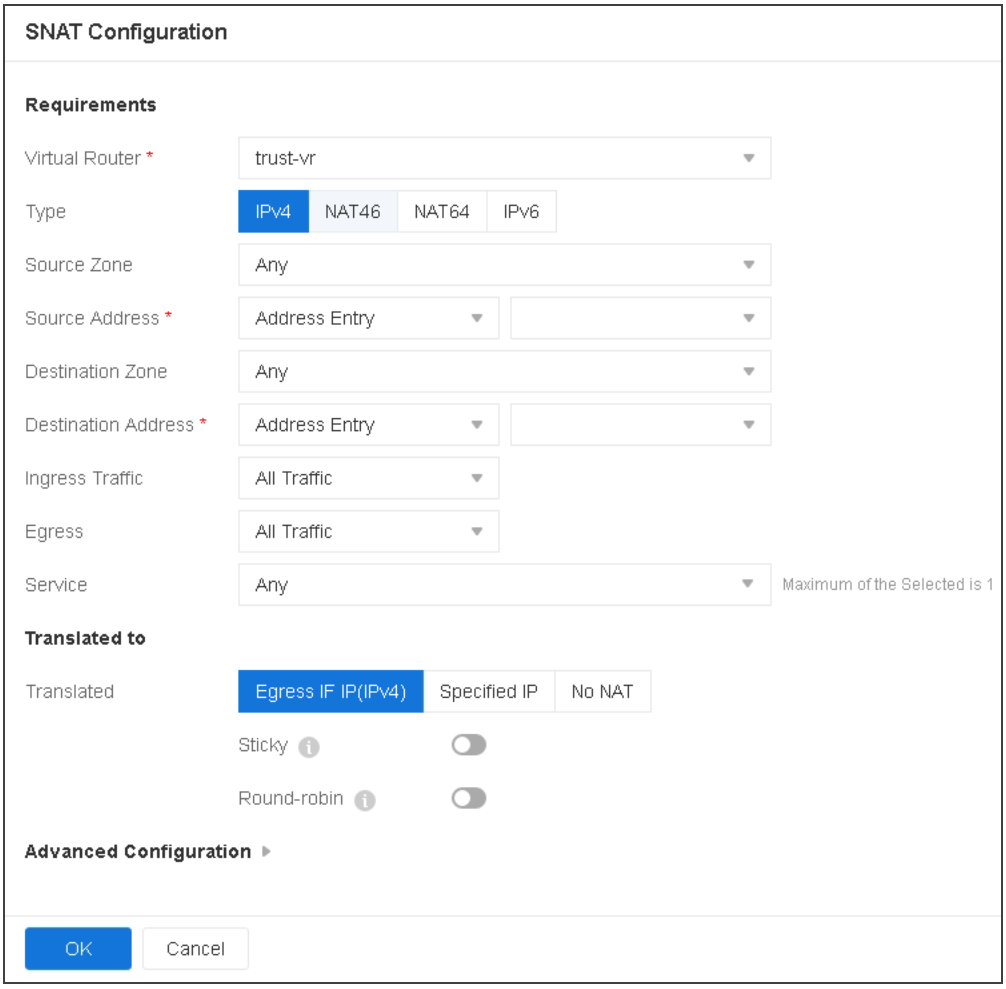
The devices achieve the NAT function through the creation and implementation of NAT rules. There are two types of NAT rules, which are source NAT rules (SNAT Rule) and destination NAT rules (DNAT Rule). SNAT translates source IP addresses, thereby hiding the internal IP addresses or sharing the limited IP addresses; DNAT translates destination IP addresses, and usually the IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device is translated to public IP addresses.

Configuring SNAT

To create an SNAT rule, take the following steps:

1. Select **Policy > NAT > SNAT**.

2. Click **New** to open the SNAT Configuration page.



In this page, configure the following options.

Requirements	
Virtual Router	Specifies a VRouter for the SNAT rule. The SNAT rule will take effect when the traffic flows into this VRouter and matches the

Requirements	
	SNAT rule conditions.
Type	Specifies the type of the SNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types of SNAT rules may vary in this page, please refer to the actual page.
Source Zone	Specifies the security zone to which the ingress interface of traffic that matches the SNAT rule is bound. By default, Any is selected. After the configuration is completed, only the traffic that flows through the ingress interface bound to this security zone can continue to match the SNAT rule. **Note:** The source zone needs to belong to the specified virtual router.
Source Address	Specifies the source IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP (IPv6) Address - Type an IP (IPv6) address into the box. Type an IPv4 address if the type of the SNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the SNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the SNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the

Requirements	
	type of the SNAT rule is NAT64 or IPv6.
Destination Address	Specifies the destination IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP (IPv6) Address - Type an IP (IPv6) address into the box. Type an IPv4 address if the type of the SNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the SNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the SNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the SNAT rule is NAT64 or IPv6.
Ingress Traffic	Specifies the ingress traffic, the default value is all traffic. • All traffic - Specifies all traffic as the ingress traffic. Traffic from any ingress interfaces will continue to match this SNAT rule. • Ingress Interface - Specifies the ingress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not.

Requirements	
Egress	Specifies the egress traffic, the default value is all traffic. • All traffic - Specifies all traffic as the egress traffic. Traffic from all egress interfaces will continue to match this SNAT rule. • Egress Interface - Specifies the egress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not. • Next Virtual Router - Specifies the next virtual router of traffic. Select a virtual router from the drop-down list.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click **New Service** or **New Group**.
Translated to	
Translated	Specifies the translated NAT IP address, including: • Egress IF IP (IPv4)/Egress IF IP (IPv6) - Specifies the NAT IP address to be an egress interface IP address. • Specified IP - Specifies the NAT IP address to be a specified IP address. After selecting this option, continue to specify the available IP address in the **Address** drop-down list. • No NAT - Do not implement NAT.

Requirements	
	The translated action for different types of SNAT rules may vary in this page, please refer to the actual page.

Mode	Specifies the translation mode, including:
	• Static - Static mode means one-to-one translation. This mode requires the translated address entry to contain the same number of IP addresses as that of the source address entry.
	• Dynamic IP - Dynamic IP mode means multiple-to-one translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied.
	• Dynamic port - Called PAT. Multiple source addresses will be translated to one specified IP address in an address entry.
	  • If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. Click the **Enable** button behind Sticky to enable Sticky.
	  • If Round-robin is enabled, all sessions from an IP address will be mapped to the same fixed IP address. Click the **Enable** button behind Round-robin to enable Round-robin.
	  • If Sticky and Round-robin are not enabled, the first

Requirements	
	address in the address entry will be used first; when the port resources of the first address are exhausted, the second address will be used. • If Track is enabled, the system will track whether the translated public address is valid, i.e., use the translated address as the source address to track if the destination website or host is accessible. The configured track object can be a Ping track object, HTTP track object, TCP track object. For more details, see "Track Object" on Page 985. This function only supports SNAT of IPv4 or NAT64 type, and the translated address should be an IP address or an address in address book, as well as the translation mode is dynamicport mode. The system will prioritize the translated address which is tracked successfully. When a translated address failed to visit a website or a host, it will be temporarily disabled until being tracked successfully again. When the tracking object fails, the system will disable the address and generate a log in the next tracking cycle, and no longer translate the private address to a public address until the address restores to reachable. If all the address in the public address book of SNAT rules are unreachable, the system will not disable any translated address and generate a log. Click the

Requirements	
	Enable button behind Track to enable the function, and select a track object from the drop-down list • NPTv6: Select the NPTv6 mode. NPTv6 (IPv6-to-IPv6 Network Prefix Translation) is described in RFC 6296 and used to implement NAT66. When this mode is selected, NPTv6 can translate an inside IPv6 source address prefix to outside IPv6 source prefix in IPv6 packet header. The translation is based on the algorithm described in RFC 6296, which serves as a useful mechanism for implementing address independence. This mode supports a larger number of address translation and reduces resource consumption by using quick address mapping. **Note**: The Sticky function and the Round-robin function are mutually exclusive and cannot be configured at the same time. **Notes:** • The NPTv6 mode is available only when the Type parameter is set to IPv6 and the Translated parameter is set to Specified IP. • The NPTv6 mode requires that both the source address of the traffic and the translated address are either "IPv6/prefix" or address from address book.

Requirements	
	 • If the source address of the traffic and the translated address are "IPv6/prefix", the IPv6 prefix needs to be 8 to 64 in length. • If the source address of the traffic and the translated address are address from address book, you can only configure one IPv6 subnet mask member whose subnet mask is 8 to 64 in length.

Expand Advanced Configuration, configure the corresponding options.

Option	Description
HA Group	Specifies the HA group that the SNAT rule belongs to. The default setting is 0.
Schedule	Specifies the schedule of the SNAT rule. Select a schedule from the drop-down list. In addition, fuzzy search is supported. To create a schedule, click ⊕.
NAT Log	Click the Enable button to enable the log function for this SNAT rule. The system will generate log information when there is traffic matching this NAT rule. **Note**: If the translated NAT IP address is an egress interface IP address, it is necessary to specify the egress interface of the traffic at the same time in order to generate logging information.
Position	Specifies the position of the rule. Each SNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the SNAT rules in order, and then implement NAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching. Select one of the following items from the drop-down list: • Bottom - The rule is located at the bottom of all the rules in the SNAT rule list. By default, system will put the newly-created SNAT rule at the bottom of all SNAT rules. • Top - The rule is located at the top of all the rules in the

Option	Description
	SNAT rule list. • Before ID - Type the ID number into the text box. The rule will be located before the ID you specified. • After ID - Type the ID number into the text box. The rule will be located after the ID you specified.
ID	Specifies the method you get the rule ID. Each rule has its unique ID. It can be automatically assigned by system or manually assigned by yourself. If you select **Manually assign** , type an ID number into the box behind.
Description	Types the description.

3. Click **OK** to save the settings.



Notes:

- When configuring a static source NAT66 rule, the minimum subnet mask must be 48 bits.
- If the SNAT rule is configured with a source zone or destination zone that is not Any, the zone cannot be deleted.

Enabling/Disabling a SNAT rule

By default the configured SNAT rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

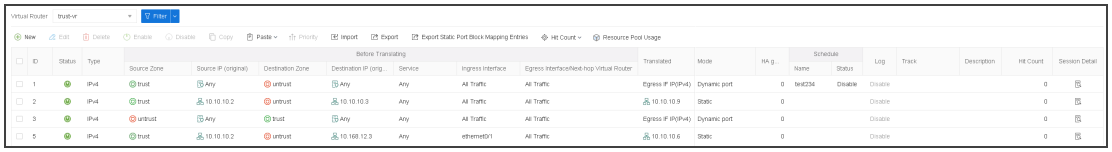
To enable/disable a SNAT rule:

1. Select **Policy > NAT > SNAT**.
2. Select the SNAT rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

Viewing and Searching SNAT Rules

You can view and search the SNAT rules on the SNAT rule list.

View the SNAT rules on the SNAT rule list.



- Each column displays the corresponding configurations. The **Schedule** column displays the name and status of SNAT rules. If **Disable** is displayed, it indicates that the SNAT rule does not take effect or has expired.
- Click icon in the Session Detail column on the SNAT rule list to go to the **Session Detail** page. You can view the current session status of the selected SNAT rule. You can also click Filter to add filtering conditions and search for the sessions that conform to the filtering conditions.

  You can filter **Session ID**, **Source Address**, **Source Port**, **Destination Address**, **Destination Port**, **Protocol**, **Application**, **Flow0 Interface**, **Flow1 Interface**. You can add multiple filter conditions at the same time. The relationship between filter conditions is **And**.
- Hover over your mouse over the configurations in different columns, then the WebUI displays either icon or the detailed information of this configuration based on the configuration type.

- You can view the detailed configurations directly.
- You can click ⋮ icon. Based on the configuration type, the WebUI displays **Filter**, **Add Filter**, or **Details**.
    - Click **Filter** or **Add Filter**, you can see the filter conditions of this configuration above the list, and then you can filter the SNAT rule according to the filter conditions.
    - Click **Details** to see the detailed configurations. Then, in the **Details** section, click **View** next to **Entry Details** to view the details about the address or service.

Adjusting Priority

Each SNAT rule has a unique ID. When the traffic flows into the device, the device will search the SNAT rules in order and then implement NAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching.

To adjust priority, take the following steps:

1. Select **Policy > NAT > SNAT**.
2. Select the rule you want to adjust its priority and click **Priority**.
3. In the Priority page, move the selected rule to:
    - Top: The rule is moved to the top of all of the rules in the SNAT rule list.
    - Bottom: The rule is moved to the bottom of all of the rules in the SNAT rule list. By default, system will put the newly-created SNAT rule at the bottom of all of the SNAT rules.
    - Before ID: Specifies an ID number. The rule will be moved before the ID you spe-

cified.

- After ID: Specifies an ID number. The rule will be moved after the ID you specified.

4. Click **OK** to save the settings.

Copying/Pasting a SNAT rule

When there are a large number of NAT rules in system, to create a NAT rule which is similar to an configured NAT rule easily, you can copy the NAT rule and paste it to the specified location.

To copy/paste a SNAT rule, take the following steps:

1. Select **Policy > NAT > SNAT**.
2. Select the SNAT rule that you want to clone and click **Copy**.
3. Click **Paste**. In the pop-up, select the desired position. Then the rule will be cloned to the desired position.
    - Top: The rule is pasted to the top of all the rules in the SNAT rule list.
    - Bottom: The rule is pasted to the bottom of all the rules in the SNAT rule list.
    - Before the Rule Selected: The rule will be pasted before the Rule being selected.
    - After the Rule Selected: The rule will be pasted after the Rule being selected.

Importing SNAT rule

You can import the configuration file of the local SNAT rules into the device to avoid creating SNAT rules manually. Only the DAT format file is supported currently.

To import the configuration file of SNAT rules, take the following steps:

1. Click **Policy** > **NAT** > **SNAT** .

2. Click the **Import** button to open the **Import** page.



3. Click **Browse** and select the local configuration file of SNAT rule to upload.

4. Click **OK**, and the imported SNAT rule will be displayed in the list.

Notes:

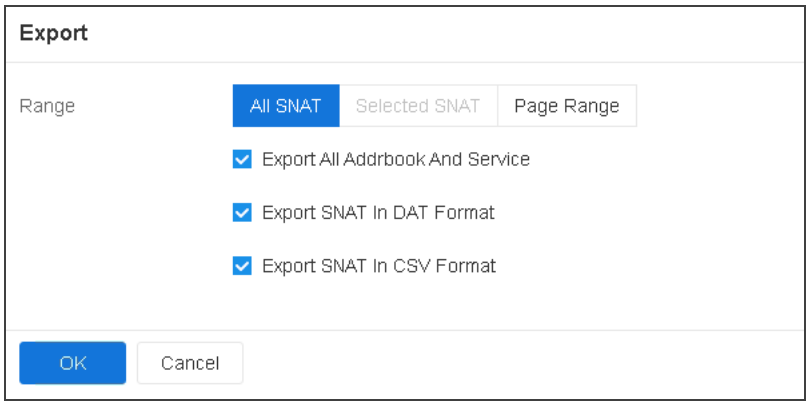
- When importing the source NAT rule configuration file, please use the exported original file as far as possible and do not modify the contents of the file. Otherwise, it may cause formatting errors.
- If there's an error during import, system will stop importing immediately and roll back configurations automatically.
- If the ID of the imported source NAT already exists, the configuration of the original NAT rule will be overwritten.
- The imported SNAT rule will be displayed on the bottom of the SNAT rule list.

Exporting SNAT rule

You can export the SNAT rules existing on the device to the local in the format of HTML CSV or DAT formats. At the same time, all the custom objects of address book and service book (only user defined)can be exported.

To export the SNAT rules, take the following steps:

1. Click **Policy** > **NAT** > **SNAT** .
2. Click **Export** to open the **Export** page.



Option	Description
Range	Specify the range of SNAT rules to be exported. • All SNAT: Select the radio button and export all SNAT rules on the device. • Selected SNAT: In the SNAT list, select the snat rule to be exported, and then click **Export** > **Selected SNAT**. • Page Range: Select the radio button, and enter the page number or page range of the SNAT list to be exported. **Note**: Separate the page number or range with semicolons, e.g. "3;5-8".
Export Address And Service	Select the check box to export all the custom objects including address book, and service book （only user defined） will be generated.
Export SNAT in DAT Format	Select the check box to export the SNAT configurations in the format of DAT.

3. Click **OK** to download the exported files. There're four kinds of files: natExport.html, " snat+exported time.zip", "snat+exported time.cvs" and the "vr_snat +exported time.dat "configurations in the DAT format.

4. Double-click the natExport.html, click **Import File** and import the " snat+exported time.zip" to view the table of exported policies.

Exporting NAT444 Static Mapping Entries

You can export the NAT444 static mapping entries to a file . The exported file contains the ID, source IP address, translated IP address, start port, end port, and the protocol information.

To export the NAT444 static mapping entries, take the following steps:

1. Select **Policy > NAT > SNAT**.

2. Click **Export NAT444 Static Mapping Entries.**

3. Select a location to store the file and click **Save**.

The exported file is CSV format. It is recommended to export the file through the management interface.

Configuring SNAT Optimization

If a large amount of NAT rules pile up in the device and you are not sure whether to delete them, this makes it more difficult to maintain these rules. The system supports the SNAT Optimization function, including hit analysis and redundancy check.

Hit Count

The system supports statistics on SNAT rule hit counts, i.e., statistics on the matching between traffic and SNAT rules. Each time the inbound traffic is matched to a certain SNAT rule, the hit count will increment by 1 automatically.

To view a SNAT rule hit count, click **Policy > NAT > SNAT**. In the SNAT rule list, view the statistics on SNAT rule hit count under the Hit Count column.

Clearing NAT Hit Count

To clear a SNAT rule hit count, take the following steps:

1. Select **Policy > NAT > SNAT Optimization**.
2. Click **Clear** to open the **Clearing NAT Hit Count** page.
    - All NAT: Clears the hit counts for all NAT rules.
    - NAT ID: Clears the hit counts for a specified NAT rule ID.
3. Click **OK**.

Hit Count Check

System supports to check SNAT rule hit counts.

To check hit count, take the following steps:

1. Select **Policy > NAT > SNAT Optimization**.
2. Click **Analyze**.

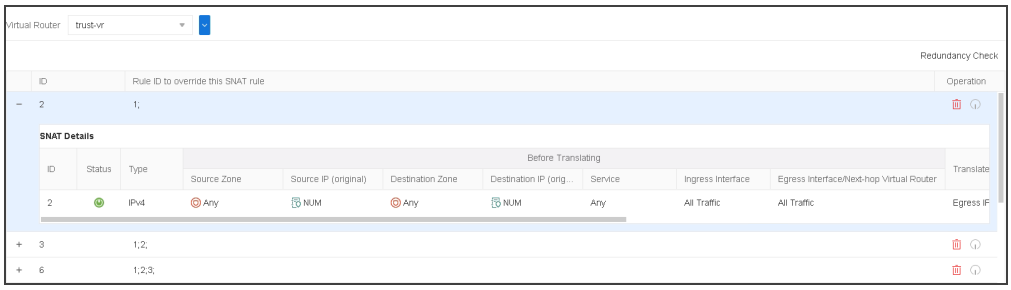
Redundancy Check

To ensure the validity of SNAT rules, the system can perform redundancy check on the SNAT rules. In other words, the system checks the coverage scope of SNAT rules to solve the problem that certain SNAT rules are overwritten and thus cannot be hit. After you complete the check, redundant SNAT rules are displayed in the redundancy check list.

To perform redundancy check on SNAT rules, take the following steps:

1. Select **Policy** > **NAT** > **SNAT Optimization**. On the **SNAT Optimization** page, click the **Redundancy Check** tab.
2. After you select a virtual router from the **Virtual Router** drop-down list and click **Redundancy Check**, the system starts to check all SNAT rules, which may take a long time. After

the check is completed, redundant SNAT rules are displayed in the list.



- The **ID** column displays the ID of SNAT rules that are overwritten and the **Rule ID to override this SNAT rule** column displays the ID of all rules that overwrite this SNAT rule.
- Find an overwritten SNAT rule and click in the **Operation** column to delete this rule.
- Find an overwritten SNAT rule and click in the **Operation** column to disable this rule. If you do not modify the status of this SNAT rule after the rule is disabled, the rule is excluded from redundancy check. To enable the SNAT rule, select **Policy** > **NAT** > **SNAT**. On the **SNAT** page, select the target SNAT rule and click **Enable**.
- Click "+" to expand the details about the overwritten SNAT rule.

Notes: After redundancy check starts, a check progress bar is displayed in the lower-left corner of the SNAT rule list. During the redundancy check, we do not recommend that you create or modify an SNAT rule. You can click , and then click **OK** in the message that appears to stop the redundancy check.

Configuring DNAT

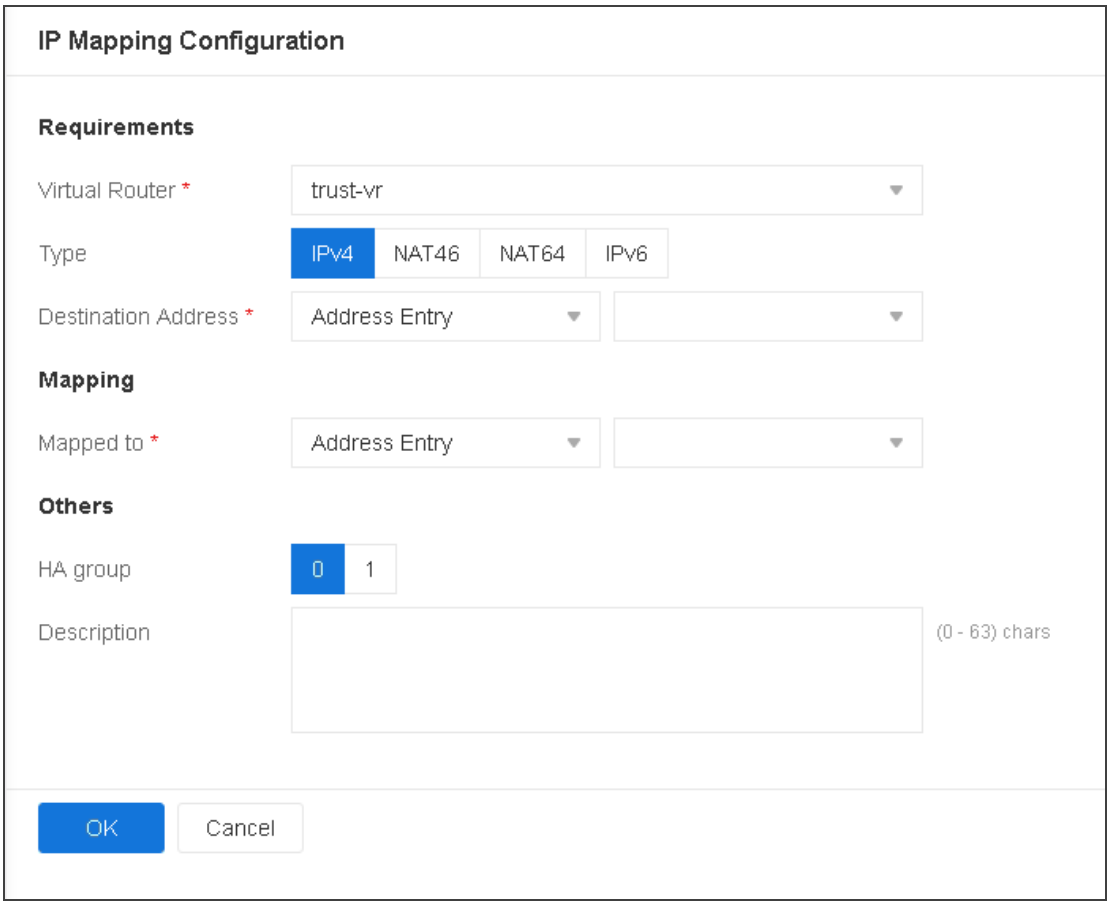
DNAT translates destination IP addresses, usually the IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device is translated to the public IP addresses.

Configuring an IP Mapping Rule

To configure an IP mapping rule, take the following steps:

1. Select **Policy > NAT > DNAT**.

2. Click **New** and select **IP Mapping**



Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Type	Specifies the type of the DNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types of DNAT rules may vary in this page, please refer to the actual page.
Destination Address	Specifies the destination IP address or interface of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP Address - Type an IP address into the box. Type an IPv4 address if the type of the DNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the DNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the DNAT rule is NAT64 or IPv6. • Dynamic IP (Physical Interface) - Select an interface which obtains IP via the DHCP and PPPoE protocols.

Requirements	
	This configuration option is available if the type of the DNAT rule is IPv4 or NAT46.
Mapping	
Mapped to	Specifies the translated NAT IP address, including **Address Entry**, **IP Address**, and **IP/Netmask** (or **IPv6/Prefix**). The number of the translated NAT IP addresses you specified must be the same as the number of the destination IP addresses of the traffic.
Others	
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Description	Types the description.

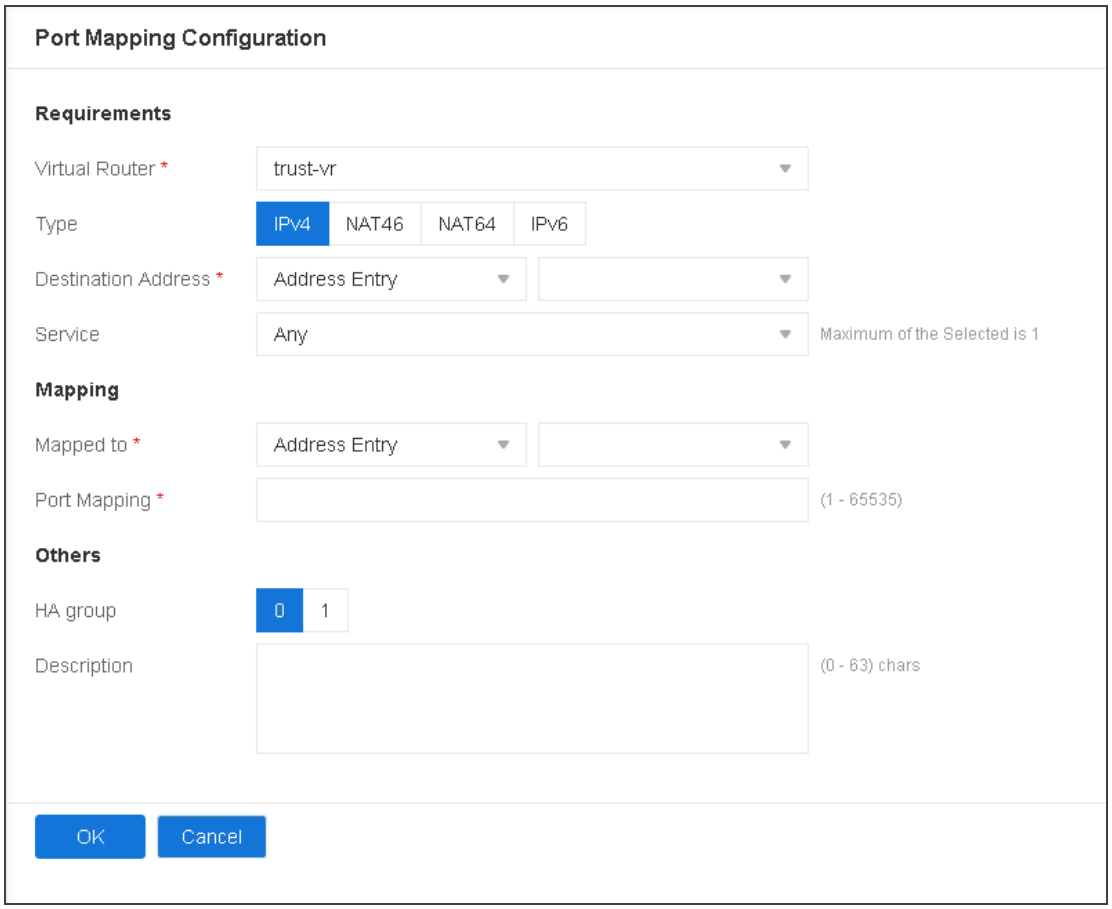
3. Click **OK** to save the settings.

Configuring a Port Mapping Rule

To configure a port mapping rule, take the following steps:

1. Select **Policy > NAT > DNAT**.

2. Click **New** and select **Port Mapping**.



Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Type	Specifies the type of the DNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types of DNAT rules may vary in this page, please refer to the actual page.
Destination Address	Specifies the destination IP address or interface of the traffic, including:

Requirements	
	• Address Entry - Select an address entry from the drop-down list. • IP Address - Type an IP address into the box. Type an IPv4 address if the type of the DNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the DNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the DNAT rule is NAT64 or IPv6. • Dynamic IP(Physical Interface) - Select an interface which obtains IP via the DHCP and PPPoE protocols. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click **New Service** or **New Group**.
Mapping	
Mapped to	Specifies the translated NAT IP address, including **Address Entry**, **IP Address**, and **IP/Netmask** (or **IPv6/Prefix**). The number of the translated NAT IP addresses you specified must be

Requirements	
	the same as the number of the destination IP addresses of the traffic.
Port Mapping	Types the translated port number of the Intranet server. The available range is 1 to 65535.
Others	
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Description	Types the description.

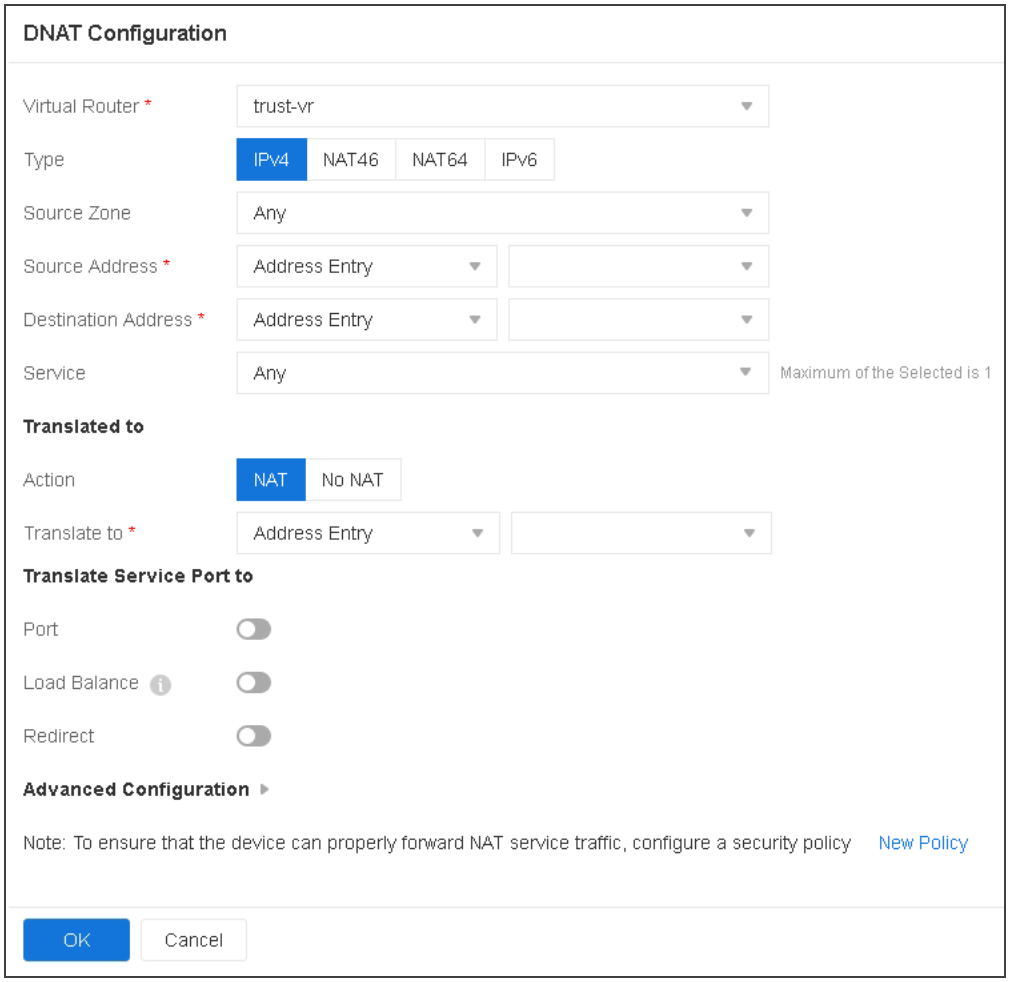
3. Click **OK** to save the settings.

Configuring an Advanced NAT Rule

You can create a DNAT rule and configure the advanced settings, or you can edit the advanced settings of an exiting DNAT rule.

To create a DNAT rule and configure the advanced settings, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Click **New** and select **Advanced Configuration**. To edit the advanced settings of an existing DNAT rule, select it and click **Edit**. The **DNAT configuration** page will appear.



In this page, configure the following options.

Requirements	
Virtual Router	Specifies a VRouter for the DNAT rule. The DNAT rule will take effect when the traffic flows into this VRouter and matches the DNAT rule conditions.
Type	Specifies the type of the DNAT rule, including IPv4, NAT46, NAT64, and IPv6. The configuration options for different types of DNAT rules may vary in this page, please refer to the actual page.

Requirements	
Source Zone	Specifies the security zone to which the ingress interface of traffic that matches the DNAT rule is bound. By default, Any is selected. After the configuration is completed, only the traffic that flows through the ingress interface bound to this security zone can continue to match the DNAT rule. **Note:** The source zone needs to belong to the specified virtual router.
Source Address	Specifies the source IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP Address - Type an IP address into the box. Type an IPv4 address if the type of the DNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the DNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the DNAT rule is NAT64 or IPv6.
Destination Address	Specifies the destination IP address or interface of the traffic, including: • Address Entry - Select an address entry from the drop-

Requirements	
	down list. • IP Address - Type an IP address into the box. Type an IPv4 address if the type of the DNAT rule is IPv4 or NAT46. Type an IPv6 address if the type of the DNAT rule is NAT64 or IPv6. • IP/Netmask - Type an IPv4 address and its netmask into the box. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46. • IPv6/Prefix - Type an IPv6 address and its prefix length into the box. This configuration option is available if the type of the DNAT rule is NAT64 or IPv6. • Dynamic IP(Physical Interface): Select an interface which obtains IP via the DHCP and PPPoE protocols. This configuration option is available if the type of the DNAT rule is IPv4 or NAT46.
Service	Specifies the service type of the traffic from the drop-down list. To create a new service or service group, click **Add**.
Translated to	
Action	Specifies the action for the traffic you specified, including: • NAT - Implements NAT for the eligible traffic. • No NAT - Do not implement NAT for the eligible traffic. • V4-MAPPED - Implements NAT for the eligible traffic,

Requirements	
	and extracts the destination IPv4 address from the destination IPv6 address of the packet directly. This configuration option is available if the type of the DNAT rule is NAT64. The **Translated to** action for different types of DNAT rules may vary in this page, please refer to the actual page.
Translate to	When selecting the **NAT** option, you need to specify the translated IP address. The options include **Address Entry**, **IP Address**, **IP/Netmask** (or **IPv6/Prefix**), and **SLB Server Pool**. The **SLB Server Pool** configure option is available if the type of the DNAT rule is IPv4 or NAT64. For more information about the SLB Server Pool, view "SLB Server Pool " on Page 904.
Translate Service Port to	
Port	Click **Enable** to translate the port number of the service that matches the conditions above.
Load Balance	Click **Enable** to enable the function. Traffic will be balanced to different Intranet servers.
Redirect	Click **Enable** to enable the function. When the number of this **Translate to** is different from the **Destination Address** of the traffic or the **Destination Address** address is **any**, you must enable the redirect function for this DNAT rule.

Expand Advanced Configuration, configure the following options.

Track Server	
HA Group	Specifies the HA group that the DNAT rule belongs to. The default setting is 0.
Source translate	Enable the function for this DNAT rule to translate source addresses, that is, bidirectional NAT. After bidirectional NAT is enabled, the device will translate both the destination address and source address of packets passing through based on the DNAT rule.
Source translate to	After the source address translation function is enabled, set the type of address after translation. Options include **Address Entry**, **IP Address** and **IP/Netmask** (IPv6/Prefix Length).
Mode	Specifies the source address translation mode, including: • Dynamic port: With this option enabled, the same source IP address will be translated to the same NAT address. If translation fails, an arbitrary NAT address will be selected. • Static port: This mode means one-to-one translation. It requires the number of source IP addresses be the same as that of NAT addresses.
Schedule	Specifies the schedule of the DNAT rule. Select a schedule from the drop-down list. In addition, fuzzy search is supported. To create a schedule, click ⊕.
Track Ping Packets	After enabling this function, system will send Ping packets to check whether the Intranet servers are reachable.
Track TCP	After enabling this function, System will send TCP packets to

Track Server	
Packets	check whether the TCP ports of Intranet servers are reachable.
TCP Port	Specifies the TCP port number of the monitored Intranet server.
NAT Log	Enable the log function for this DNAT rule to generate the log information when traffic matches this NAT rule.
Position	Specifies the position of the rule. Each DNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the DNAT rules by sequence, and then implement DNAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the DNAT rule list is the order of the rule matching. Select one of the following items from the drop-down list: • Bottom - The rule is located at the bottom of all of the rules in the DNAT rule list. By default, the system will put the newly-created DNAT rule at the bottom of all of the DNAT rules. • Top - The rule is located at the top of all of the rules in the DNAT rule list. • Before ID - Type the ID number into the text box. The rule will be located before the ID you specified. • After ID - Type the ID number into the text box. The rule will be located after the ID you specified.
ID	The ID number is used to distinguish between NAT rules. Specifies the method you get the rule ID. It can be automatically

Track Server	
	assigned by system or manually assigned by yourself.
Description	Types the description.

3. Click **OK** to save the settings.

> **Notes:** If the DNAT rule is configured with a source zone that is not Any, the zone cannot be deleted.

Enabling/Disabling a DNAT Rule

By default the configured DNAT rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

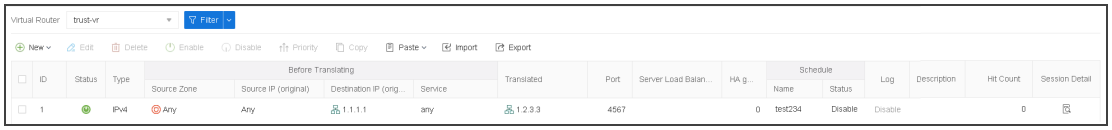
To enable/disable a policy rule, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Select the DNAT rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

Viewing and Searching DNAT Rules

You can view and search the DNAT rules on the DNAT rule list.

View the DNAT rules on the DNAT rule list.



- Each column displays the corresponding configurations. The **Schedule** column displays the name and status of DNAT rules. If **Disable** is displayed, it indicates that the DNAT rule does not take effect or has expired.
- Click  icon in the Session Detail column on the DNAT rule list to go to the **Session Detail** page. You can view the current session status of the selected DNAT rule. You can also click 

to add filtering conditions and search for the sessions that conform to the filtering conditions.

  You can filter **Session ID**, **Source Address**, **Source Port**, **Destination Address**, **Destination Port**, **Protocol**, **Application**, **Flow0 Interface**, **Flow1 Interface**. You can add multiple filter conditions at the same time. The relationship between filter conditions is **And**.
- Hover over your mouse over the configurations in different columns, then the WebUI displays either icon or the detailed information of this configuration based on the configuration type.
  - You can view the detailed configurations directly.
  - You can click icon. Based on the configuration type, the WebUI displays **Filter**, **Add Filter**, or **Details**.
    - Click **Filter** or **Add Filter**, you can see the filter conditions of this configuration above the list, and then you can filter the DNAT rule according to the filter condition.
    - Click **Details** to see the detailed configurations. Then, in the **Details** section, click **View** next to **Entry Details** to view the details about the address or service.

Copying/Pasting a DNAT Rule

When there are a large number of NAT rules in system, to create a NAT rule which is similar to an configured NAT rule easily, you can copy the NAT rule and paste it to the specified location.

To copy/paste a DNAT rule, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Select the DNAT rule that you want to clone and click **Copy**.
3. Click **Paste**. In the pop-up, select the desired position. Then the rule will be cloned to the desired position.
    - Top: The rule is pasted to the top of all of the rules in the DNAT rule list.
    - Bottom: The rule is pasted to the bottom of all of the rules in the DNAT rule list.
    - Before the Rule Selected: The rule will be pasted before the Rule selected.
    - After the Rule Selected: The rule will be pasted after the Rule selected.

Adjusting Priority

Each DNAT rule has a unique ID. When the traffic is flowing into the device, the device will search the DNAT rules in order, and then implement NAT of the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the DNAT rule list is the order of the rule matching.

To adjust priority, take the following steps:

1. Select **Policy > NAT > DNAT**.
2. Select the rule you want to adjust its priority and click **Priority**.

3. In the Priority page, move the selected rule to:

    - Top: The rule is moved to the top of all of the rules in the DNAT rule list.
    - Bottom: The rule is moved to the bottom of all of the rules in the DNAT rule list. By default, system will put the newly-created DNAT rule at the bottom of all of the DNAT rules.
    - Before ID: Specifies an ID number. The rule will be moved before the ID you specified.
    - After ID: Specifies an ID number. The rule will be moved after the ID you specified.

4. Click **OK** to save the settings.

Importing DNAT rule

You can import the configuration file of the local DNAT rules into the device to avoid creating DNAT rules manually. Only the DAT format file is supported currently.

To import the configuration file of DNAT rules, take the following steps:

1. Click **Policy** > **NAT** > **DNAT** .
2. Click the **Import** button to open the **Import** page.



3. Click **Browse** and select the local configuration file of DNAT rule to upload.
4. Click **OK**, and the imported DNAT rule will be displayed in the list.

Notes:

- When importing the source NAT rule configuration file, please use the exported original file as far as possible and do not modify the contents of the file. Otherwise, it may cause formatting errors.
- If there's an error during import, system will stop importing immediately and roll back configurations automatically.
- If the ID of the imported source NAT already exists, the configuration of the original NAT rule will be overwritten.
- The imported DNAT rule will be displayed on the bottom of the DNAT rule list.

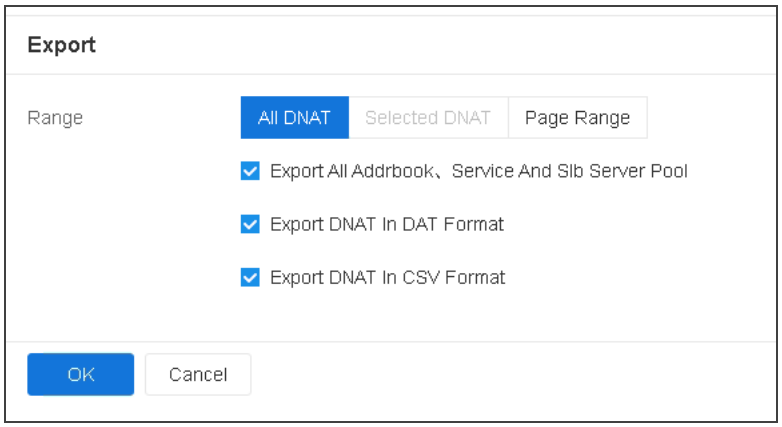
Exporting DNAT rule

You can export the DNAT rules existing on the device to the local in the format of HTML CSV or DAT formats. At the same time, all the custom objects of address book , service book (only user defined) and slb server (only user defined) can be exported.

To export the DNAT rules, take the following steps:

1. Click **Policy** > **NAT** > **DNAT** .

2. Click **Export** to open the **Export** page.



Option	Description
Range	Specify the range of DNAT rules to be exported. • All DNAT: Select the radio button and export all DNAT rules on the device. • Selected DNAT: In the DNAT list, select the DNAT rule to be exported, and then click **Export** > **Selected DNAT**. • Page Range: Select the radio button, and enter the page number or page range of the DNAT list to be exported. **Note**: Separate the page number or range with semicolons, e.g. "3;5-8".
Export Address, Service And Slb Server Pool	Select the check box to export all the custom objects including address book, service book （only user defined） and slb server (only user defined) will be generated.
Export DNAT in DAT Format	Select the check box to export the DNAT configurations in the format of DAT.

3. Click **OK** to download the exported files. There're four kinds of files: natExport.html, " dnat+exported time.zip", "dnat+exported time.cvs" and the "vr_dnat +exported time.dat "configurations in the DAT format.

4. Double-click the natExport.html, click **Import File** and import the " dnat+exported time.zip" to view the table of exported policies.

Configuring DNAT Optimization

If a large amount of NAT rules pile up in the device and you are not sure whether to delete them, this makes it more difficult to maintain these rules. The system supports the DNAT Optimization function, including hit analysis and redundancy check.

Hit Count

The system supports statistics on DNAT rule hit counts, i.e., statistics on the matching between traffic and DNAT rules. Each time the inbound traffic is matched to a certain DNAT rule, the hit count will increment by 1 automatically.

To view a DNAT rule hit count, click **Policy > NAT > DNAT**. In the DNAT rule list, view the statistics on DNAT rule hit count under the Hit Count column.

Clearing NAT Hit Count

To clear a DNAT rule hit count, take the following steps:

1. Select **Policy > NAT > DNAT Optimization**.

2. Click **Clear** to open the **Clearing NAT Hit Count** page.

   - All NAT: Clears the hit counts for all NAT rules.

   - NAT ID: Clears the hit counts for a specified NAT rule ID.

3. Click **OK**.

Hit Count Check

System supports to check policy rule hit counts.

To check hit count, take the following steps:

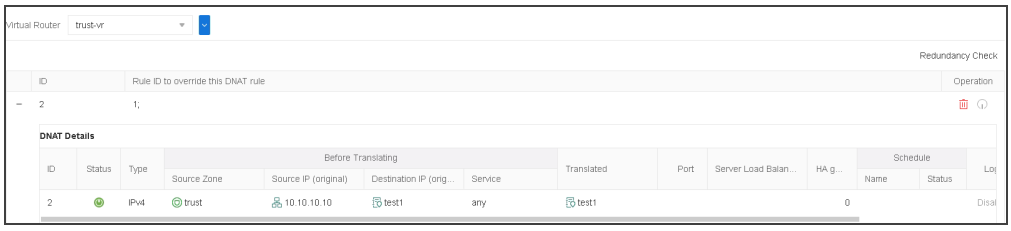
1. Select **Policy > NAT > DNAT Optimization**.
2. Click **Analyze**.

Redundancy Check

To ensure the validity of DNAT rules, the system can perform redundancy check on the DNAT rules. In other words, the system checks the coverage scope of DNAT rules to solve the problem that certain DNAT rules are overwritten and thus cannot be hit. After you complete the check, redundant DNAT rules are displayed in the redundancy check list.

To perform redundancy check on DNAT rules, take the following steps:

1. Select **Policy** > **NAT** > **DNAT Optimization**. On the **DNAT Optimization** page, click the **Redundancy Check** tab.
2. After you select a virtual router from the **Virtual Router** drop-down list and click **Redundancy Check**, the system starts to check all DNAT rules, which may take a long time. After the check is completed, redundant DNAT rules are displayed in the list.



- The **ID** column displays the ID of DNAT rules that are overwritten and the **Rule ID to override this DNAT rule** column displays the ID of all rules that overwrite this DNAT rule.

- Find an overwritten DNAT rule and click  in the **Operation** column to delete this rule.
- Find an overwritten DNAT rule and click  in the **Operation** column to disable this rule. If you do not modify the status of this DNA3T rule after the rule is disabled, the rule is excluded from redundancy check. To enable the DNAT rule, select **Policy** > **NAT** > **DNAT**. On the **DNAT** page, select the target DNAT rule and click **Enable**.
- Click "+" to expand the details about the overwritten DNAT rule.



Notes: After redundancy check starts, a check progress bar is displayed in the lower-left corner of the DNAT rule list. During the redundancy check, we do not recommend that you create or modify a DNAT rule. You can click , and then click **OK** in the message that appears to stop the redundancy check.

Configuring DNS Rewrite

When the client sends a DNS resolution request to the public DNS server through the firewall, the system can rewrite the IP address in the response message returned by the DNS server to a private IP address based on DNS rewrite rules. This protects and hides networking environment configuration.

You can set multiple DNS rewrite rules, which are matched in descending order. The system uses the first rule that the response message matches to rewrite the IP address. You can view the order of DNS rewrite rules on the **Policy** > **NAT** > **DNS Rewrite** page.

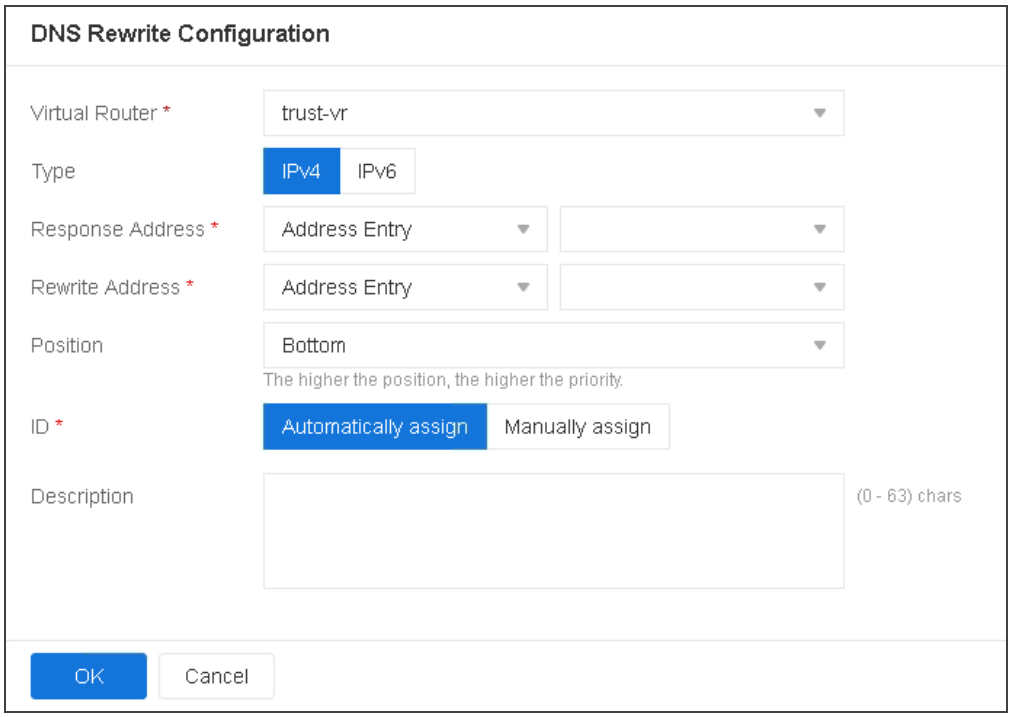


Notes: After enabling the DNS ALG function, the DNS rewrite function will take effect. For detailed information on how to enable DNS ALG, please refer to "Application Layer Gateway (ALG)" on Page 339.

Configuring a DNS Rewrite Rule

To configure a DNS rewrite rule, take the following steps:

1. Select **Policy** > **NAT** > **DNS Rewrite**.
2. Click **New**.



Option	Description
Virtual Router	Specifies the virtual router to which the DNS rewrite rule belongs.
Type	Specifies the IP protocol of the DNS rewrite rule. Valid values: IPv4 and IPv6.
Response Address	Specifies the address to be rewritten, which can be an address entry, IP address, IP/netmask, or host book. For Address Entry or Host Book, you can select a configured address entry or host

Option	Description
	book, or create one.
Rewrite Address	Specifies the address after the rewrite operation, which can be an address entry, IP address, or IP/netmask. For Address Entry, you can select a configured address entry or create one.
Position	Specifies the position of the DNS rewrite rule, which can be placed before or after a specified ID, or can be placed at the first or last position. By default, a newly created rule is placed at the end of all rules.
ID	Specifies the ID of the DNS rewrite rule. Each rule has a unique ID. The ID can be automatically assigned by the system or you can manually assign one. Valid values: 1 to 16.
Description	Enter a description for the DNS rewrite rule. It can be up to 63 characters in length.

3. Click **OK**.

Managing DNS Rewrite Rules

To view configured DNS rewrite rules, select **Policy** > **NAT** > **DNS Rewrite**.

- To modify a DNS rewrite rule, select this rule from the list and click **Edit**.
- To delete one or more DNS rewrite rules, select these rules from the list and click **Delete**.
- To adjust the order of a DNS rewrite rule, select this rule from the list and click **Priority**.
- To filter DNS rewrite rules, click **Filter**, select a filter type from the drop-down list, and then enter a filter condition.

Viewing Dynamic Mapping Table of DNS Rewrite

The dynamic mapping table of DNS rewrite stores the mappings between the response address and the rewrite address. After a DNS response is received, the system obtains the domain name and IP address from the response and searches for dynamic mapping entries in the table.

- If a dynamic mapping entry is matched, the DNS response is directly rewritten and the TTL of the dynamic mapping entry is updated.
- If no dynamic mapping entry is matched, DNS rewrite rules are matched in descending order of priority. If a DNS rewrite rule is matched, the system generates a dynamic mapping entry and rewrites the DNS response. If no DNS rewrite rule is matched, the system directly forwards the DNS response.

After a business access request is received from the client, the system searches for a matched entry in the dynamic mapping table and performs NAT based on the matched entry.

Select **Policy** > **NAT** > **DNS Rewrite Dynamic Mapping** to view the dynamic mapping table of DNS rewrite stored in the system. You can click **Filter** to specify filter conditions based on your needs.

SLB Server

View SLB server status: After you enabling the track function (PING track, TCP track, or UDP track), system will list the status and information of the intranet servers that are tracked.

View SLB server pool status: After you enabling the server load balancing function, system will monitor the intranet servers and list the corresponding status and information.

Viewing SLB Server Status

To view the SLB server status, take the following steps:

1. Select **Policy > NAT > SLB Server Status**.
2. You can set the filtering conditions according to the virtual router, SLB server pool, and server address and then view the information.

Option	Description
Server	Shows the IP address of the server.
Type	Shows the type of the server, include IPv4 or IPv6.
Port	Shows the port number of the server.
Status	Shows the status of the server.
Current Sessions	Shows the number of current sessions.
DNAT	Shows the DNAT rules that uses the server.
HA Group	Shows the HA group that the server belongs to.

Viewing SLB Server Pool Status

To view the SLB server pool status, take the following steps:

1. Select **Policy > NAT > SLB Server Pool Status**.

2. You can set the filtering conditions according to the virtual router, algorithm, and server pool name and then view the information.

Option	Description
Name	Shows the name of the server pool name.
Type	Shows the type of the server pool, include IPv4 or IPv6.
Algorithm	Shows the algorithm used by the server pool.
DNAT	Shows the DNAT rules that use the server.
Abnormal Server/All Servers	Shows the number of abnormal servers and the total number of the servers.
Current Sessions	Shows the number of current sessions.

iQoS

System provides iQoS (intelligent quality of service) which guarantees the customer's network performance, manages and optimizes the key bandwidth for critical business traffic, and helps the customer greatly in fully utilizing their bandwidth resources.

iQoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. iQoS can assure the normal transmission of critical business traffic when the network is overloaded or congested. iQoS is controlled by license. To use iQoS, apply and install the iQoS license.

Notes: If you have configured QoS in the previous QoS function before upgrading the system to verion 5.5, the previous QoS function will take effect. You still need to configure the previous QoS function in CLI. You cannot use the newest iQoS function in version 5.5 and the newest iQoS function will not display in the WebUI



and will not take effect. If you have not configured the previous QoS function before upgrading the system to version 5.5, the system will enable the newest iQoS function in version 5.5. You can configure iQoS function in the WebUI and the previous QoS function will not take effect.

Implement Mechanism

The packets are classified and marked after entering system from the ingress interface. For the classified and marked traffic, system will smoothly forward the traffic through the shaping mechanism, or drop the traffic through the policing mechanism. If the shaping mechanism is selected to forward the traffic, the congestion management and congestion avoidance mechanisms will give different priorities to different types of packets so that the packets of higher priority can pass though the gateway earlier to avoid network congestion.

In general, implementing QoS includes:

- Classification and marking mechanism: Classification and marking is the process of identifying the priority of each packet. This is the first step of iQoS.
- Policing and shaping mechanisms: Policing and shaping mechanisms are used to identify traffic violation and make responses. The policing mechanism checks the traffic in real time and takes immediate actions according to the settings when it discovers a violation. The shaping mechanism works together with queuing mechanism. It makes sure that the traffic will never exceed the defined flow rate so that the traffic can go through that interface smoothly.
- Congestion management mechanism: Congestion management mechanism uses the queuing theory to solve problems in the congested interfaces. As the data rate can be different among different networks, congestion may happen to both wide area network (WAN) and local area network (LAN). Only when an interface is congested will the queuing theory begin to work.

- Congestion avoidance mechanism: Congestion avoidance mechanism is a supplement to the queuing algorithm, and it also relies on the queuing algorithm. The congestion avoidance mechanism is designed to process TCP-based traffic.

Pipes and Traffic Control Levels

System supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes.

Pipes

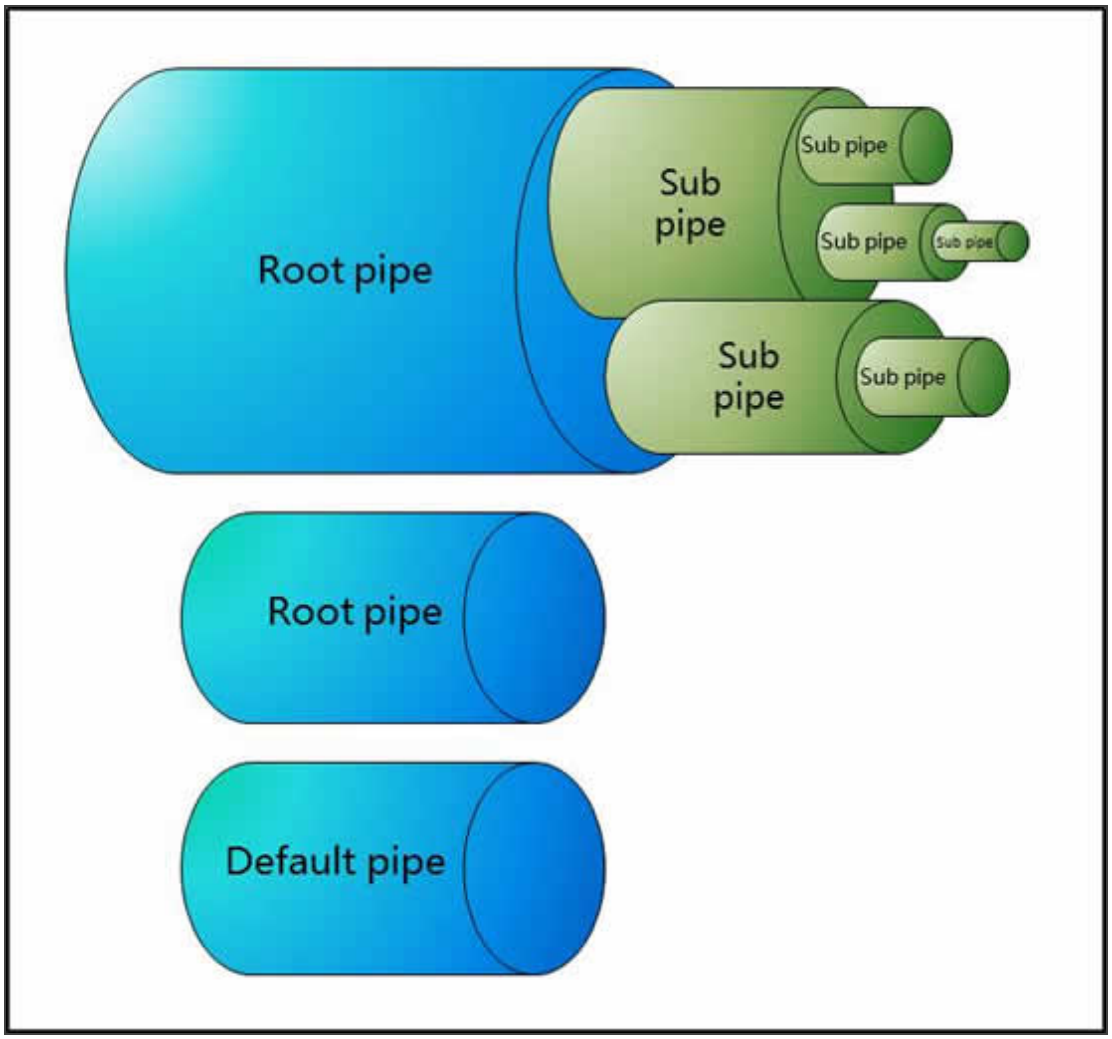
By configuring pipes, the devices implement iQoS. Pipe, which is a virtual concept, represents the bandwidth of transmission path. System classifies the traffic by using the pipe as the unit, and controls the traffic crossing the pipes according to the actions defined for the pipes. For all traffic crossing the device, they will flow into virtual pipes according to the traffic matching conditions they match. If the traffic does not match any condition, they will flow into the default pipe pre-defined by the system.

Pipes, except the default pipe, include two parts of configurations: traffic matching conditions and traffic management actions:

- Traffic matching conditions: Defines the traffic matching conditions to classify the traffic crossing the device into matched pipes. System will limit the bandwidth to the traffic that matches the traffic matching conditions. You can define multiple traffic matching conditions to a pipe. The logical relation between each condition is OR. When the traffic matches a traffic matching condition of a pipe, it will enter this pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list in the Policy > iQoS page.
- Traffic management actions: Defines the actions adopted to the traffic that has been classified to a pipe. The data stream control includes the forward control and the backward control. For-

ward control controls the traffic that flows from the source to the destination; backward control controls the traffic flows from the destination to the source.

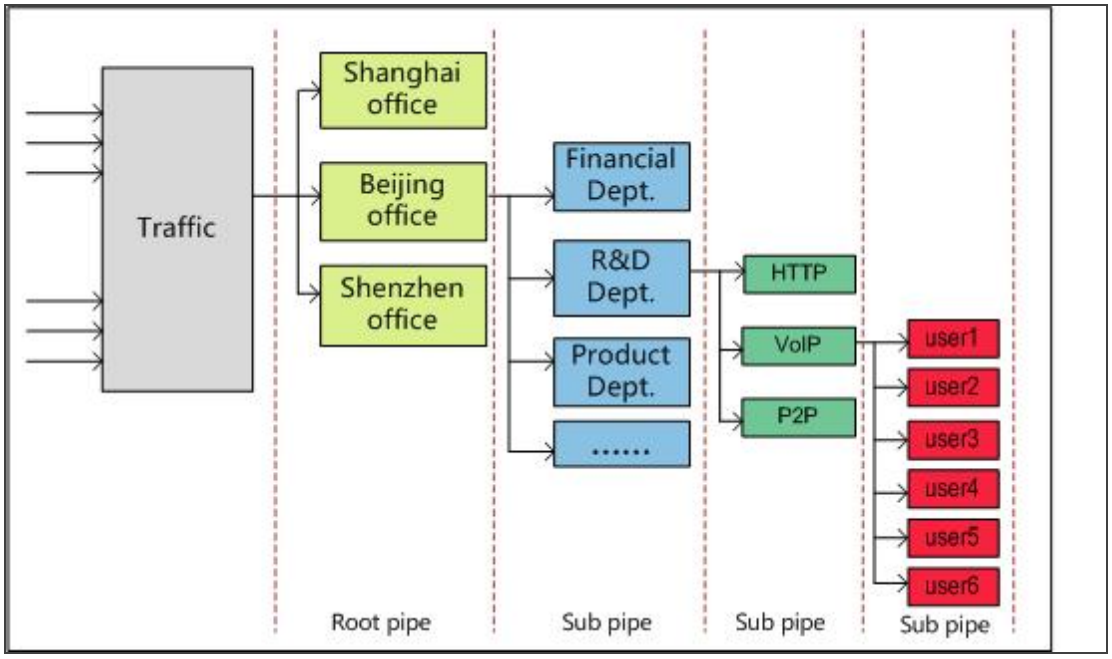
To provide flexible configurations, system supports the multiple-level pipes. Configuring multiple-level pipes can limit the bandwidth of different applications of different users. This can ensure the bandwidth for the key services and users. Pipes can be nested to at most four levels. Sub pipes cannot be nested to the default pipe. The logical relation between pipes is shown as below:



- You can create multiple root pipes that are independent. At most three levels of sub pipes can be nested to the root pipe.
- For the sub pipes at the same level, the total of their minimum bandwidth cannot exceed the minimum bandwidth of their upper-level parent pipe, and the total of their maximum bandwidth cannot exceed the maximum bandwidth of their upper-level parent pipe.
- If you have configured the forward or backward traffic management actions for the root pipe, all sub pipes that belong to this root pipe will inherit the configurations of the traffic direction set on the root pipe.
- The root pipe that is only configured the backward traffic management actions cannot work.

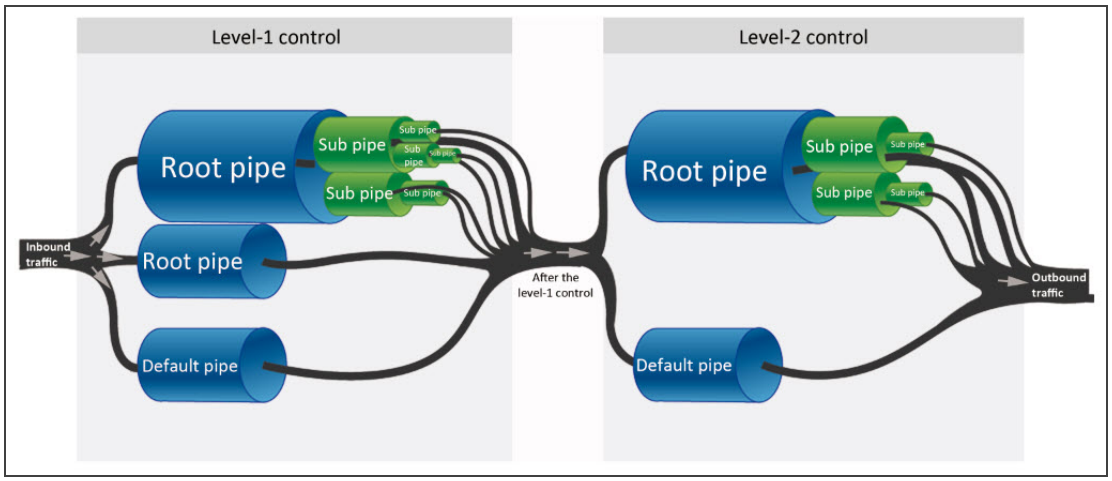
The following chart illustrates the application of multiple-level pipes in a company. The administrator can create the following pipes to limit the traffic:

1. Create a root pipe to limit the traffic of the office located in Beijing.
2. Create a sub pipe to limit the traffic of its R&D department.
3. Create a sub pipe to limit the traffic of the specified applications so that each application has its own bandwidth.
4. Create a sub pipe to limit the traffic of the specified users so that each user owns the defined bandwidth when using the specified application.



Traffic Control Levels

System supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes. Traffic that is dealt with by level-1 control flows into the level-2 control, and then system performs the further management and control according to the pipe configurations of level-2 control. After the traffic flowing into the device, the process of iQoS is shown as below:



According to the chart above, the process of traffic control is described below:

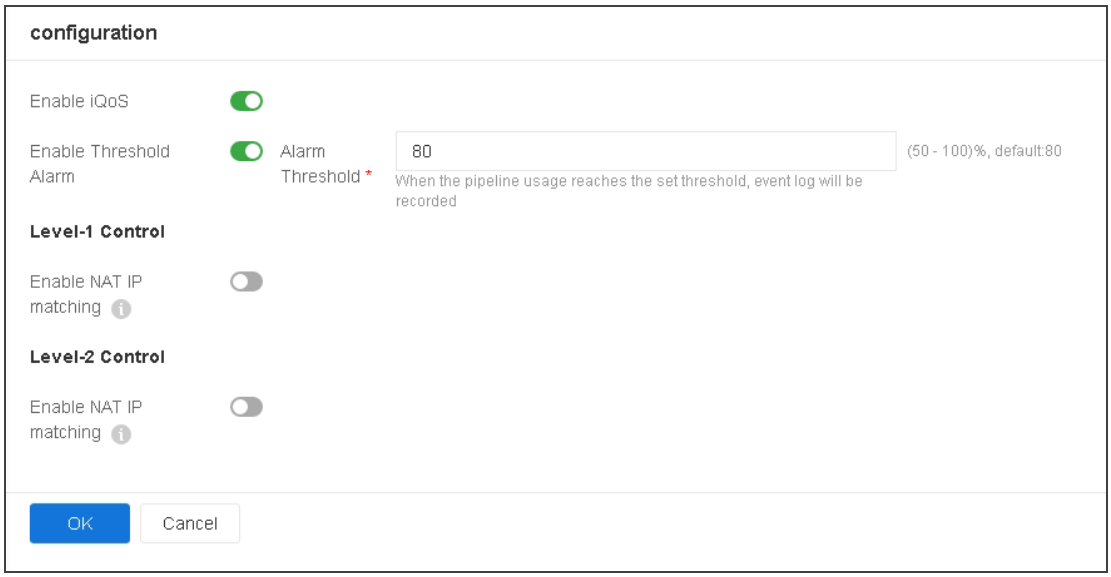
1. The traffic first flows into the level-1 control, and then system classifies the traffic into different pipes according to the traffic matching conditions of the pipe of level-1 control. The traffic that cannot match any pipe will be classified into the default pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list in the **Policy > iQoS** page. After the traffic flows into the root pipe, system classifies the traffic into different sub pipes according to the traffic matching conditions of each sub pipe.
2. According to the traffic management actions configured for the pipes, system manages and controls the traffic that matches the traffic matching conditions.
3. The traffic dealt with by level-1 control flows into the level-2 control. System manages and controls the traffic in level-2 control. The principles of traffic matching, management and control are the same as the one of the level-1 control.
4. Complete the process of iQoS.

Enabling iQoS

To enable iQoS, take the following steps:

1. Select **Policy > iQoS > Configuration**.

2. Click the **Enable iQoS** button.



3. Select the **Enable Threshold Alarm** checkbox, and specify the alarm threshold in the **Alarm Threshold** textbox. The range is from 50 to 100. The default value is 80. After the function is enabled and the alarm threshold is specified, when the pipeline usage reaches or exceeds the specified alarm threshold, the system will record a warning level event log. For the same pipeline, the system records the event log at an interval of 10 seconds.

4. If you click the **Enable NAT IP matching** button in **Level-1 Control** or **Level-2 Control**, system will use the IP addresses between the source NAT and the destination NAT as the matching items. If the matching is successful, system will limit the speed of these IP addresses.

> **Notes:** Before enabling NAT IP matching, you must config the NAT rules. Otherwise, the configuration will not take effect.

5. Click **Apply** to save the configurations.

Pipes

By using pipes, devices implement iQoS. Pipes in different traffic control levels will take effect in different stages.

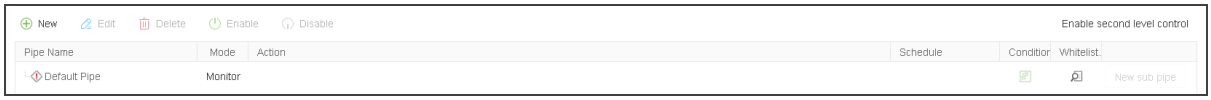
Configuring pipes includes the following sections:

1. Create the traffic matching conditions, which are used to capture the traffic that matches these conditions. If configuring multiple traffic matching conditions for a pipe, the logical relation between each condition is OR.
2. Create a white list according to your requirements. System will not control the traffic in the white list. Only root pipe and the default pipe support the white list.
3. Specify the traffic management actions, which are used to deal with the traffic that is classified into a pipe.
4. Specify the schedule. The pipe will take effect during the specified time period.

Notes:

Basic Operations

Select **Policy > iQoS > Policy** to open the Policy page.



You can perform the following actions in this page:

- Disable the level-2 traffic control: Click **Disable second level control**. The pipes in the level-2 traffic control will not take effect. The Level-2 Control tab will not appears in this page.
- View pipe information: The pipe list displays the name, mode, action, schedule, and the description of the pipes.

- Click the icon to expand the root pipe and display its sub pipes.
- Click the icon of the root pipe or the sub pipe to view the condition settings.
- Click the icon of the root pipe to view the white list settings.
- represents the root pipe is usable, represents the root pipe is unusable, represents the sub pipe is usable, represents the sub pipe is unusable,

  Default Pipe the gray text represents the pipe is disabled.

- Create a root pipe: Select the Level-1 Control or Level-2 Control tab, then click **New** in the menu bar to create a new root pipe.
- Create a sub pipe: Click the icon of the root pipe or the sub pipe to create the corresponding sub pipe.
- Click **Enable** in the menu bar to enable the selected pipe. By default, the newly-created pipe will be enabled.
- Click **Disable** in the menu bar to disable the selected pipe. The disabled pipe will not take effect.
- Click **Delete** to delete the selected pipe. The default pipe cannot be deleted.

Configuring a Pipe

To configure a pipe, take the following steps:

1. According to the methods above, create a root pipe or sub pipe. The Pipe Configuration page appears.

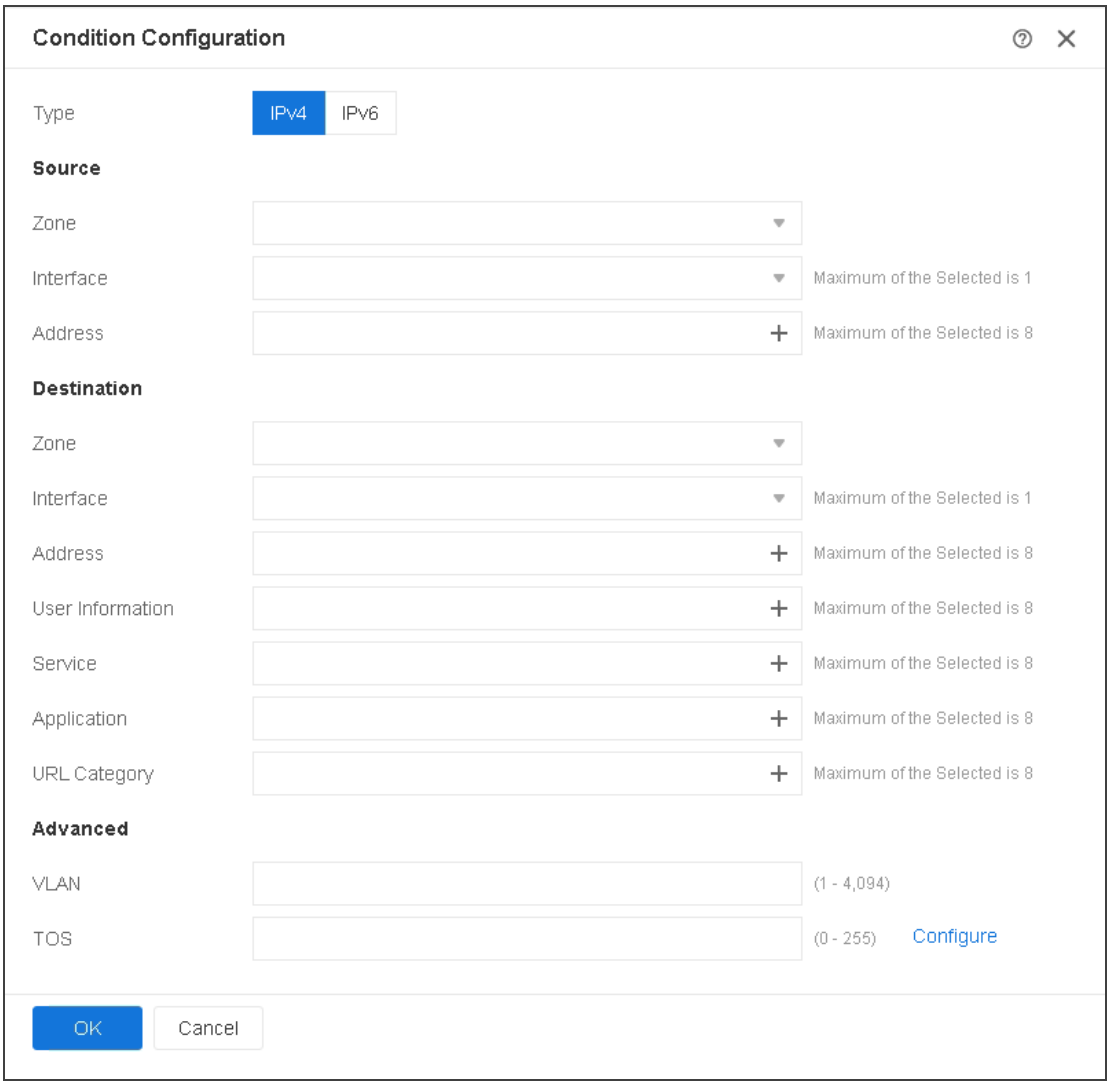
2. In this page, specify the basic pipe information.

Option	Description
Parent Pipe/Control Level	Displays the control level or the parent pipe of the newly created pipe.
Pipe Name	Specify a name for the new pipe.

Mode	Shape, Policy, or Stat.
	• The Shape mode can limit the data transmission rate and smoothly forward the traffic. This mode supports the bandwidth borrowing and priority adjusting for the traffic within the root pipe.
	• The Policy mode will drop the traffic that exceeds the bandwidth limit. This mode does not support the bandwidth borrowing and priority adjusting, and cannot guarantee the minimum bandwidth.
	  • Bandwidth borrowing: All of the sub pipes in a root pipe can lend their idle bandwidth to the pipes that are lacking bandwidth. The prerequisite is that their bandwidth must be enough to forward the traffic in their pipes.
	  • Priority adjusting: When there is traffic congestion, system will arrange the traffic to enter the waiting queue. You can set the traffic to have higher priority and system will deal with the traffic in order of precedence.
	• The Stat mode will monitor the matched traffic, generate the statistics, and will not control the traffic.

Option	Description
Description	Specify the description of this pipe.
Schedule	Specifies a schedule when the pipe will take effect. Select a desired **schedule** from the Schedule drop-down list. **Notes**: Please check the associated schedule in each pipe configuration to avoid the situation where the effective sub-pipe bandwidth exceeds the root pipe configuration during a certain period, which may cause abnormal operation of iQos.

3. In Condition, click **New**.



Option	Description
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type IP. If IPv6 is selected, all the IP/netmask, IP range, address entry configured should be in the IPv6 format.
Source Information	
Zone	Specify the source zone of the traffic. Select the zone name from

Option	Description
	the drop-down menu.
Interface	Specify the source interface of the traffic. Select the interface name from the drop-down menu. **Notes:** iQoS does not support to configure a tunnel interface. To limit the speed of tunnel traffic, use the method of policy-based IPSec VPN. For more information, see "Configuring an IPSec VPN" on Page 558。
Address	Specify the source address of the traffic. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click **Add** to add the addresses to the left pane. 4. After adding the desired addresses, click **Close** to complete the address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ to create a new address entry. • You can click ▾ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety

Option	Description
	of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched.
Destination Information	
Zone	Specify the destination zone of the traffic. Select the zone name from the drop-down menu.
Interface	Specify the destination interface of the traffic. Select the interface name from the drop-down menu.
Address	Specify the destination address of the traffic. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click **Add** to add the addresses to the right pane. 4. After adding the desired addresses, click **Close** to com-

Option	Description
	plete the address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click ⊕ to create a new address entry. • You can click ▾ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched.
User Information	Specify a user or user group that the traffic belongs to. 1. From the **User** drop-down menu, select the AAA server where the users and user groups reside.

Option	Description
	2. Based on different types of AAA server, you can execute one or more actions: search a user/user group/role, expand the user/user group list, and enter the name of the user/user group. 3. After selecting users/user groups/roles, click them to add them to the left pane. 4. After adding the desired objects, click **Close** to complete the user information configuration.
Service	Specify a service or service group that the traffic belongs to. 1. From the **Service** drop-down menu, select a type: Service, Service Group. 2. You can search the desired service/service group, expand the service/service group list. 3. After selecting the desired services/service groups, click them to add them to the right pane. 4. After adding the desired objects, click **Close** to complete the service configuration. You can also perform other operations: • To add a new service or service group, select **User-defined** from the "Predefined" drop-down list, and click ⊕. • The default service configuration is any. To restore the configuration to this default one, select the **any** check box.

Option	Description
Application	Specify an application, application group, or application filters that the traffic belongs to. 1. From the **Application** drop-down menu, you can search the desired application/application group/application filter, expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click them to add them to the left pane. 3. After adding the desired objects, click **Close** complete the application configuration. You can also perform other operations: • To add a new application group, click ⊕. • To add a new application filter, click ⊕. **Note**: Deprecated predefined applications cannot be added.
URL Category	Specifies the URL category that the traffic belongs to. After the user specifies the URL category, the system matches the traffic according to the specified category. 1. In the "URL category" drop-down menu, the user can select one or more URL categories, up to 8 categories. 2. After selecting the desired filters, click the blank area in this page to complete the configuration.

Option	Description
	To add a new URL category, click ⊕ , the page will pop up "URL category" page. In this page, the user can configure the category name and URL.
Advanced	
VLAN	Specify the VLAN information of the traffic.
TOS	Specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the TOS Configuration page. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum cost. • Reserved: Specify the normal service.
TrafficClass	Specify the TOS fields of the traffic.

4. If you are configuring root pipes, you can specify the white list settings based on the description of configuring conditions.

5. Configuring the trigger threshold for the maximum floating bandwidth.

Option	Description
Lower threshold of a	Specifies the lower threshold of the bandwidth utilization for a root pipe. When the bandwidth utilization is lower than the

Option	Description
root pipe's bandwidth utilization	lower threshold, the maximum floating bandwidth of sub pipes is triggered. The value range is 20%-75%. The default lower threshold is 40%.
Upper threshold of a root pipe's bandwidth utilization	Specifies the upper threshold of the bandwidth utilization for a root pipe. When the bandwidth utilization is higher than the upper threshold, the maximum floating bandwidth of sub pipes will not be triggered. The value range is 76%-90%. The default lower threshold is 80%.

6. In Action, configuring the corresponding actions.

Forward (From source to destination)	
The following configurations control the traffic that flows from the source to the destination. For the traffic that matches the conditions, system will perform the corresponding actions.	
Pipe Bandwidth	When configuring the root pipe, specify the pipe bandwidth. When configuring the sub pipe, specify the maximum bandwidth and the minimum bandwidth of the pipe: • Min Bandwidth: Specify the minimum bandwidth. If you want this minimum bandwidth to be reserved and cannot be used by other pipes, select **Enable Reserved Bandwidth**. • Max Bandwidth: Specify the maximum bandwidth.
Limit type	Specify the maximum bandwidth and minimum bandwidth of the pipe for each user/IP:

	• Type: Select the type of the bandwidth limitation: **No Limit**, **Limit Per IP**, or **Limit Per User**.
	  • **No Limit** represents that system will not limit the bandwidth for each IP or each user.
	  • **Limit Per IP** represents that system will limit the bandwidth for each IP. In the Limit by section, select **Source IP** to limit the bandwidth of the source IP in this pipe; or select **Destination IP** to limit the bandwidth of the destination IP in this pipe.
	  • **Limit Per User** represents that system will limit the bandwidth for each user. In the Limit by section, specify the minimum/maximum bandwidth of the users.
	• When configuring the root pipe, you can select the **Enable Average Bandwidth** check box to make each source IP, destination IP, or user to share an average bandwidth.

Limit by	When the Limit type is **Limit Per IP** or **Limit Per User**, you need to specify the minimum bandwidth or the maximum bandwidth: • Min Bandwidth: Specify the minimum bandwidth. • Max Bandwidth: Specify the maximum bandwidth. • Maximum Floating Bandwidth: Specifies the maximum floating bandwidth.

	• Delay: Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
Advanced	
Priority	Specify the priority for the pipes. Select a number, between 0 and 7, from the drop-down menu. The smaller the value is, the higher the priority is. When a pipe has higher priority, system will first deal with the traffic in it and borrow the extra band-width from other pipes for it. The priority of the default pipe is 7.
TOS	Specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the appeared TOS Configuration page. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum monetary cost. • Reserved: Specify the normal service.
TrafficClass	Specifies the value of the TrafficClass field for IPv6 traffic, The TrafficClass field value of IPv6 traffic matching successfully will be set to the specified value.

Limit Opposite Bandwidth	Click the **Enable** button to configure the value of limit-strength.The smaller the value, the smaller the limit.
Backward (From condition's destination to source)	
The following configurations control the traffic that flows from the destination to the source. For the traffic that matches the conditions, system will perform the corresponding actions.	
Pipe Bandwidth	When configuring the root pipe, specify the pipe bandwidth. When configuring the sub pipe, specify the maximum bandwidth and the minimum bandwidth of the pipe: • Min Bandwidth: Specify the minimum bandwidth. If you want this minimum bandwidth to be reserved and cannot be used by other pipes, select **Enable Reserved Bandwidth**. • Max Bandwidth: Specify the maximum bandwidth.
Limit type	Specify the maximum bandwidth and minimum bandwidth of the pipe for each user/IP: • Type: Select the type of the bandwidth limitation: **No Limit**, **Limit Per IP**, or **Limit Per User**. • **No Limit** represents that system will not limit the bandwidth for each IP or each user. • **Limit Per IP** represents that system will limit the bandwidth for each IP. In the Limit by section, select **Source IP** to limit the bandwidth of the source IP in this pipe; or select **Destination IP** to

	limit the bandwidth of the destination IP in this pipe. • **Limit Per User** represents that system will limit the bandwidth for each user. In the Limit by section, specify the minimum/maximum bandwidth of the users. • When configuring the root pipe, you can click the **Enable Average Bandwidth** button to make each source IP, destination IP, or user to share an average bandwidth.
Limit by	When the Limit type is **Limit Per IP** or **Limit Per User**, you need to specify the minimum bandwidth or the maximum bandwidth: • Min Bandwidth: Specify the minimum bandwidth. • Max Bandwidth: Specify the maximum bandwidth. • Maximum Floating Bandwidth: Specifies the maximum floating bandwidth. • Delay： Specify the delay time, whose value ranges from 1 second to 3600 seconds. The maximum bandwidth limit of each IP/ user is not effective within the delay time range.
Advanced	
Priority	Specify the priority for the pipes. Select a number, between 0 and 7, from the drop-down menu. The smaller the value is, the higher the priority is. When a pipe has higher priority, system

	will first deal with the traffic in it and borrow the extra bandwidth from other pipes for it. The priority of the default pipe is 7.
TOS	Specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the appeared TOS Configuration page. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum monetary cost. • Reserved: Specify the normal service.
Limit Opposite Bandwidth	Click the **Enable** button to configure the value of limit-strength.The smaller the value, the smaller the limit.

7. Click **OK** to save the settings.

Searching QoS Policy

Use the Filter to search for the QoS policy rules that match the filter conditions.

1. Click **Policy > iQoS> Policy**, and at the top-right corner of the page, click **Filter**. Then a new row appears at the top.
2. Click **Filter** to add a new filter condition. Then select a filter condition from the drop-down menu and enter a value.
3. Press **Enter** to search for the QoS policy rules that matches the filter conditions.

4. Repeat the above two steps to add more filter conditions. The relationship between each filter condition is **AND**.

5. To delete a filter condition, hover your mouse on that condition and then click ✕ icon. To close the filter, click ✕Remove All icon on the right side of the row.

Viewing Statistics of Pipe Monitor

To view the statistics of pipe monitor, see "iQoS" on Page 1225.

Session Limit

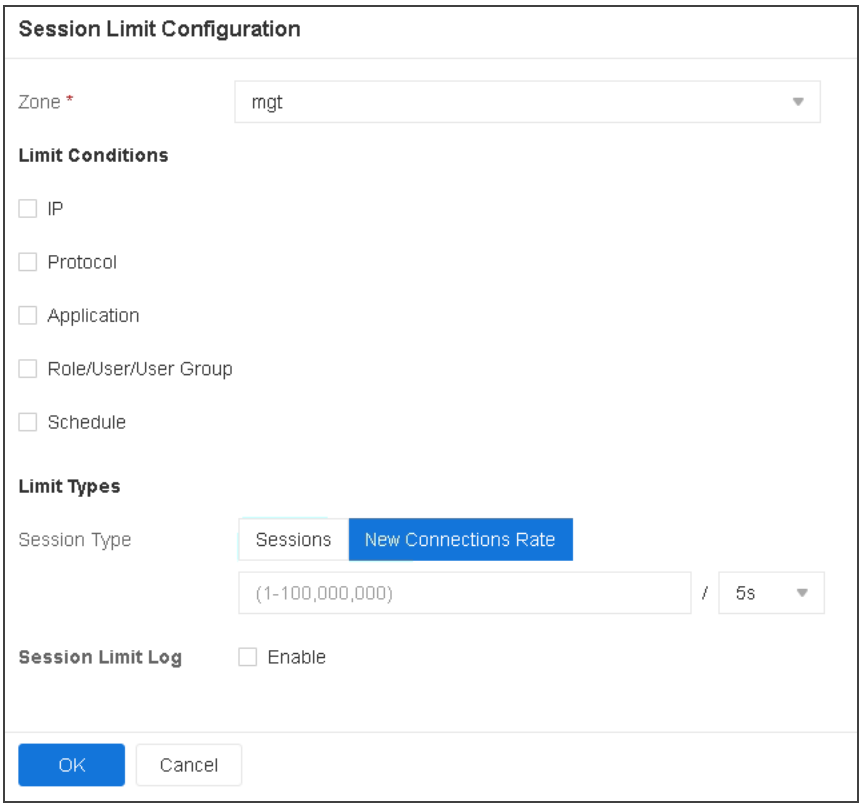
The devices support zone-based session limit function. You can limit the number of sessions and control the session rate to the source IP address, destination IP address, specified IP address, applications or role/user/user group, thereby protecting from DoS attacks and controlling the bandwidth of applications, such as IM or P2P.

Configuring Session Limit

Configuring a Session Limit Rule

To configure a session limit rule, take the following steps:

1. Select **Policy > Session Limit**.
2. Click **New**. The Session Limit Configuration page will appear.



3. Select the zone where the session limit rule is located.

4. Configure the limit conditions. a

IP	
Select the **IP** check box to configure the IP limit conditions.	
IP	Select the **IP** radio button and then select an IP address entry. • Select **All IPs** to limit the total number of sessions to all IP addresses. • Select **Per IP** to limit the number of sessions to each IP address.
Source IP-->Destination IP	Select the **Source IP-->Destination IP** radio button and specify the source IP address entry and destination IP address entry. When the session's source IP and destination IP are both within the specified range, system will limit the number of session as follows: • When you select **Per Source IP**, system will limit the number of sessions to each source IP address. • When you select **Per Destination IP**, system will limit the number of sessions to each destination IP address.
Protocol	
Protocol	Limits the number of sessions to the protocol which has been set in the text box.
Application	
Application	Limits the number of sessions to the selected application.

IP	
	Note: Deprecated predefined applications cannot be added.
Role/User/User Group	
Select the **Role/User/User Group** check box to configure the corresponding limit conditions.	
Role	Select the **Role** radio button and a role from the **Role** drop-down list to limit the number of sessions of the selected role.
User	Select the **User** radio button and a user from the **User** drop-down list to limit the number of sessions of the selected user.
User Group	Select the **User Group** radio button and a user group from the **User Group** drop-down list to limit the number of sessions of the selected user group. • Next to the **User Group** radio button, select **All Users** to limit the total number of sessions to all of the users in the user group. • Next to the **User Group** radio button, select **Per User** to limit the number of sessions to each user.
Schedule	
Schedule	Select the **Schedule** check box and choose a schedule you need from the drop-down list to make the session limit rule take effect within the time period specified by the schedule.

5. Configure the limit types.

Session Type	
Sessions	Specify the maximum number of sessions. The value of 0 indic-

Session Type	
	ates no limitation.
New Connections Rate	Specify the limit of new session rate. That is, specify the time granularity and maximum number of sessions. From the drop-down list, select 1s/5s and enter the maximum number of sessions that can be created within the specified time granularity in the field. The value ranges from 1 to 100000000.

6. Select the **Enable** after **Session Limit Log** to record the session limit log.
7. Click **OK** to save your settings.
8. Click **Switch Mode** to select a matching mode. If you select **Use the Minimum Value** and an IP address matches multiple session limit rules, the maximum number of sessions of this IP address is limited to the minimum number of sessions of all matched session limit rules; if you select **Use the Maximum Value** and an IP address matches multiple session limit rules, the maximum number of sessions of this IP address is the maximum number of sessions of all matched session limit rlules.

Clearing Statistic Information

After configuring a session limit rule, the sessions which exceed the maximum number of sessions will be dropped. You can clear the statistical information of the dropped sessions of specified session limit rule according to your need.

To clear statistic information, take the following steps:

1. Select **Policy > Session Limit**.
2. Select the rule whose session's statistical information you want to clear.
3. Click **Clear**.

Traffic Quota

System supports the traffic quota function, which can limit and control the allowable flow quota of users/user groups per day or per month. When the user traffic reaches the daily or monthly quota defined by the traffic quota profile, the system will block the user traffic.

Related Topics:

- "Configuring the Traffic Quota Rule" on Page 1256
- "Configuring the Traffic Quota Profile" on Page 1258
- "Configuring the Traffic Quota Zone" on Page 1259
- "User Quota Monitor" on Page 1527

Configuring the Traffic Quota Rule

The traffic quota rule configuration including configuring user/ user group traffic quota rule and adjusting the traffic quota rule position.

Configuring the User/ User Group Traffic Quota Rule

To configure the user/ user group traffic quota rule, take the following steps:

1. Select **Policy > Traffic Quota > Rule**.
2. In the **User Quota Rule** or **User Group Quota Rule** tab, click **New**.



In the <User Traffic Quota Rule Configuration> or <User Group Traffic Quota Rule Configuration> page, configure the corresponding options.

Option	Description
Name	Specifies the name of user/ user group traffic quota rule.
Quota Profile	Select the created quota profile from the drop-down list, or click ⊕ to create a new traffic quota profile. For traffic quota profile configuration, see "Configuring the Traffic Quota Profile" on Page 1258.
User/ User	Specifies the user/ user group of traffic quota rule.

Option	Description
Group	1. From the **User** or **User Group** drop-down list, select the AAA server where the users and user groups reside. 2. Based on the type of AAA server, you can execute one or more actions: search a user/user group, expand the user/user group list, enter the name of the user/user group. 3. After selecting users/user groups/roles, click them to add the them to the left pane. 4. After adding the desired objects, click **Close** to complete the user configuration.

3. Click **OK** to save your settings.

Adjusting Traffic Quota Rule Priority

To adjust the rule priority, take the following steps:

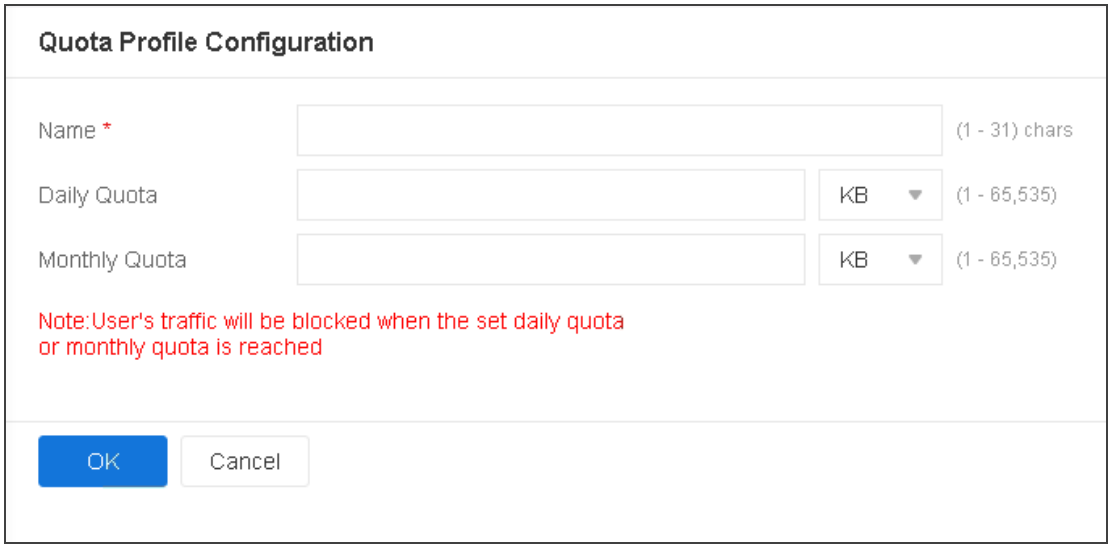
1. Select **Policy > Traffic Quota > Rule**.
2. Select the check box of the traffic quota rule whose priority will be adjusted, and click **Priority** .
3. In the **Change User Quota Rule Priority**or **Change User Group Quota Rule Priority** page, click **First List** , **Last List** , **Before This Name** or **After This Name**. Then the rule will be moved before or after the specified name.

Configuring the Traffic Quota Profile

To configure the traffic quota profile, use the following steps:

1. Select **Policy > Traffic Quota > Profile**.

2. Click **New**to open the Quota Profile Configuration page.



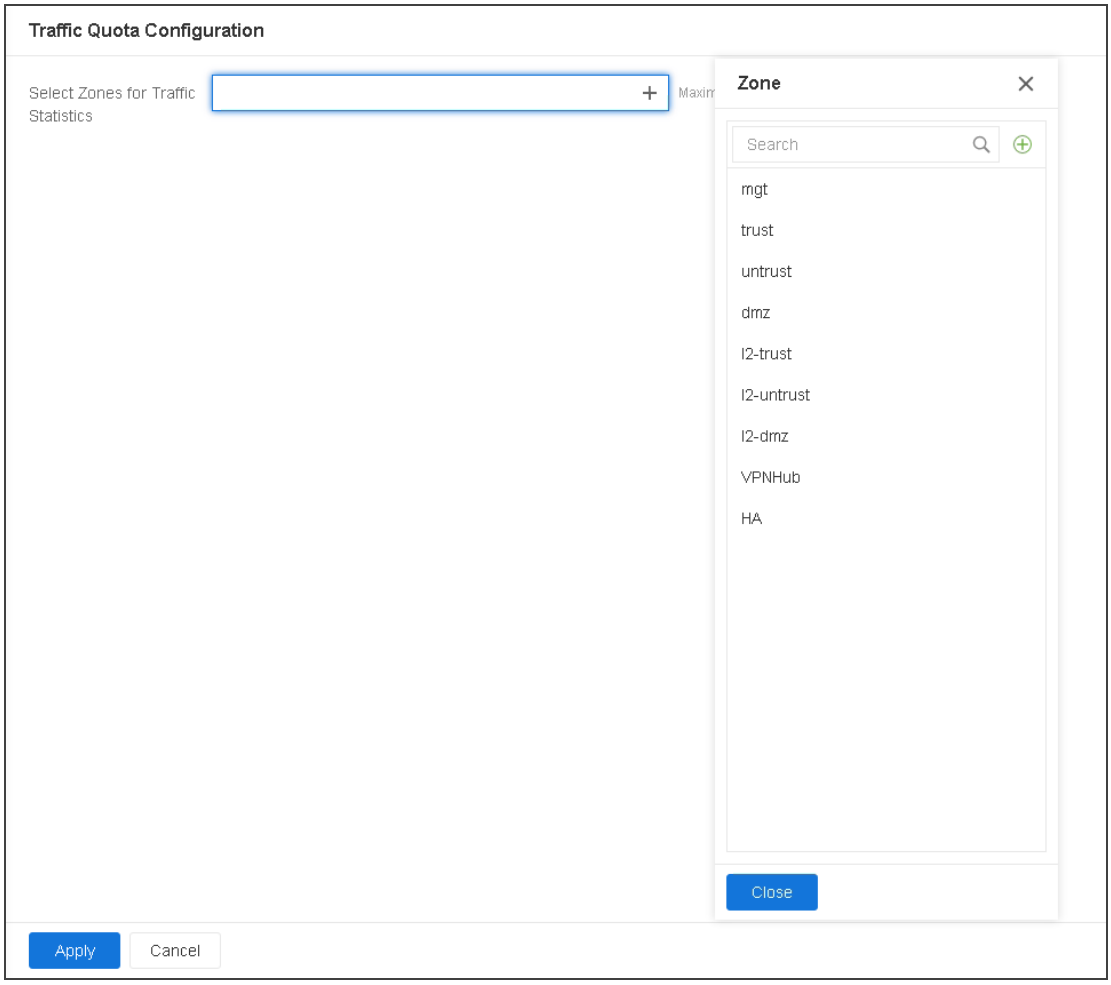
Option	Description
Name	Specifies the quota profile name.
Daily Quota	Type the daily quota in the text box and select the quota unit in the drop-down list, including KB, MB, GB, TB.
Monthly Quota	Type the monthly quota in the text box and select the quota unit in the drop-down list, including KB, MB, GB, TB.

3. Click **OK** to save your settings.

Configuring the Traffic Quota Zone

To configure the zone that you want to enable the traffic quota function, take the following steps:

1. Select **Policy > Traffic Quota > Configuration**.
2. Click **Select Zones for Traffic Statistics**.



3. Click ⊕ to add a new zone entry to the **Selected** list.
4. In the **Selected** list, select the zone entry and click ✕ for the zone entry not be counted.
5. Click **Apply** to save your settings.

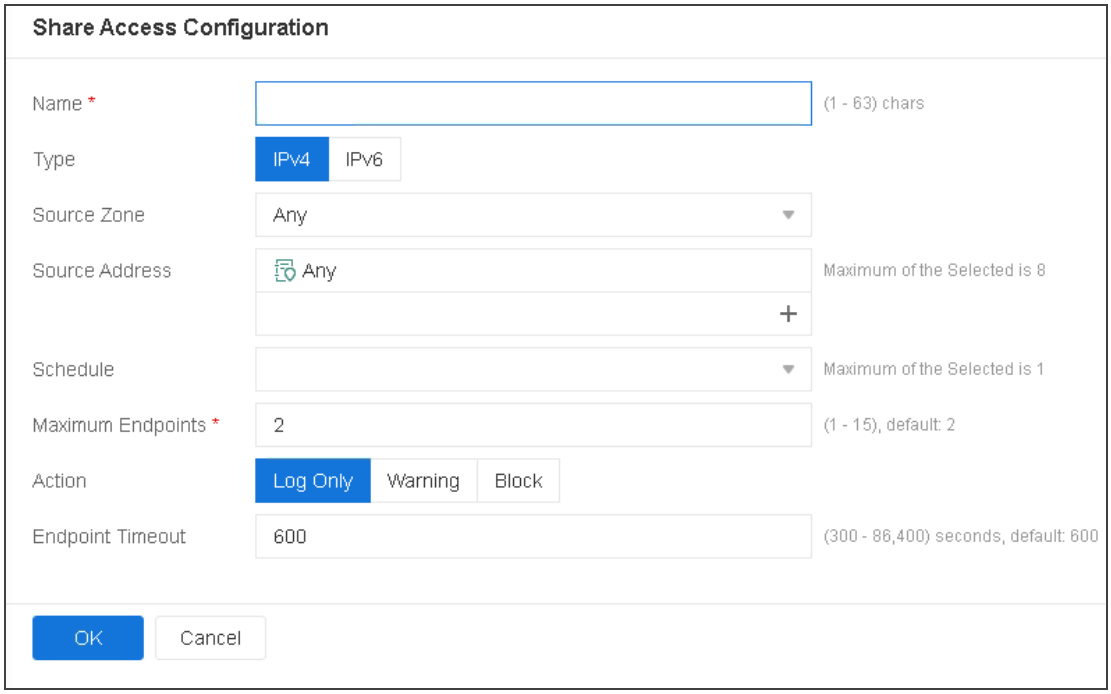
Share Access

Share access means multiple endpoints access network with the same IP. The function of share access can block access from unknown device and allocate bandwidth for users, so as to prevent possible risks and ensure good online experience.

Configuring Share Access Rules

To configure a share access rule, take the following steps:

1. Select **Policy > Share Access**.
2. Click **New**. The Share Access Configuration page will appear.



Option	Description
Name	Specifies the name of share access rule.
Source Zone	Specify the source zone of share access.
Source	Specify the source IP address segment of share access.

Option	Description
Address	1. Click + to open the **Address** page. 2. Select the address type in the **Address** page. 3. According to different address types, select or enter the required address. 4. Click **Add** to add the addresses to the left pane. 5. After adding the desired addresses, click **Close** to complete the source address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click + icon to create a new address entry. • You can click ▼ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation. In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that

Option	Description
	contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched. • The default address configuration is any. To restore the configuration to this default one, select the **any** or **IPv6-any** check box.
Schedule	Specify the schedule of share access. The share access rule takes effect in the period specified by the schedule. If the schedule is not configured, the share access rule will always be effective.
Maximum Endpoints	Specify the maximum number of share access endpoints. The range is 1-15. The default value is 2.
Action	When the number of endpoints with the same IP address exceeds the maximum allowed to be shared by system, the IP address of the endpoints will be processed according to the specified action. • Log Only: When the number of shared access endpoints exceeds the maximum, system will only record logs of the IP address out of limit, without affecting the normal connection of the access endpoints. • Warning: When the number of shared access endpoints exceeds the maximum, system will send warnings to endpoints out of limit and record logs during the specified control duration.

Option	Description
	• Control Duration: Specify the control duration of warning. The range is 30-3600s. The default value is 60s. After the duration is over, the system will re-detect whether the number of access endpoints exceeds the maximum. • Warning Message: Specify the user-defined warning message, the range is 0-255 characters. • Block: When the number of shared access endpoints exceeds the maximum, system will block the IP address of the endpoints out of the limit and record logs during the specified control duration. • Control Duration: Specify the control duration of block. The range is 30-3600s. The default value is 60s. After the duration is over, the system will re-detect whether the number of access endpoints exceeds the maximum.
Endpoint Timeout	Specify the timeout time of endpoint. After the timeout time, when the endpoint no longer accesses network with the IP, system will clear the endpoint information. The range is 300-86400s. The default value is 600s.

ARP Defense

StoneOS provides a series of ARP defense functions to protect your network against various ARP attacks, including:

- ARP Learning: Devices can obtain IP-MAC bindings in an Intranet from ARP learning, and add them to the ARP list. By default this function is enabled. The devices will always keep ARP learning on, and add the learned IP-MAC bindings to the ARP list. If any IP or MAC address changes during the learning process, the devices will add the updated IP-MAC binding to the ARP list. If this function is disabled, only IP addresses in the ARP list can access the Internet.
- MAC Learning: Devices can obtain MAC-Port bindings in an Intranet from MAC learning, and add them to the MAC list. By default this function is enabled. The devices will always keep MAC learning on, and add the learned MAC-Port bindings to the MAC list. If any MAC address or port changes during the learning process, the devices will add the updated MAC-Port binding to the MAC list.
- IP-MAC-Port Binding: If IP-MAC, MAC-Port or IP-MAC-Port binding is enabled, packets that are not matched to the binding will be dropped to protect against ARP spoofing or MAC address list attacks. The combination of ARP and MAC learning can achieve the effect of "real-time scan + static binding", and make the defense configuration more simple and effective.
- ARP Inspection: Devices support ARP Inspection for interfaces. With this function enabled, StoneOS will inspect all ARP packets passing through the specified interfaces, and compare the IP addresses of the ARP packets with the static IP-MAC bindings in the ARP list and IP-MAC bindings in the DHCP Snooping list.

- DHCP Snooping: With this function enabled, system can create a binding relationship between the MAC address of the DHCP client and the allocated IP address by analyzing the packets between the DHCP client and server.
- Host Defense: With this function enabled, the system can send gratuitous ARP packets for different hosts to protect them against ARP attacks.

Configuring ARP Defense

Configuring Binding Settings

Devices support IP-MAC binding, MAC-Port binding and IP-MAC-Port binding to reinforce network security control. The bindings obtained from ARP/MAC learning and ARP scan are known as dynamic bindings, and those manually configured are known as static bindings.

Adding a Static IP-MAC-Port Binding

To add a static IP-MAC-Port binding, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Click **New**.



Option	Description
MAC	Specify a MAC address.
IP	Specify an IP address.
Port	Select a port from the drop-down list behind.
Virtual Router	Select the virtual router that the binding item belongs to. By

Option	Description
	default, the binding item belongs to trust-vr.
Description	Specify the description for this item.

3. Click **OK** to save the settings.

Obtaining a Dynamic IP-MAC-Port Bindings

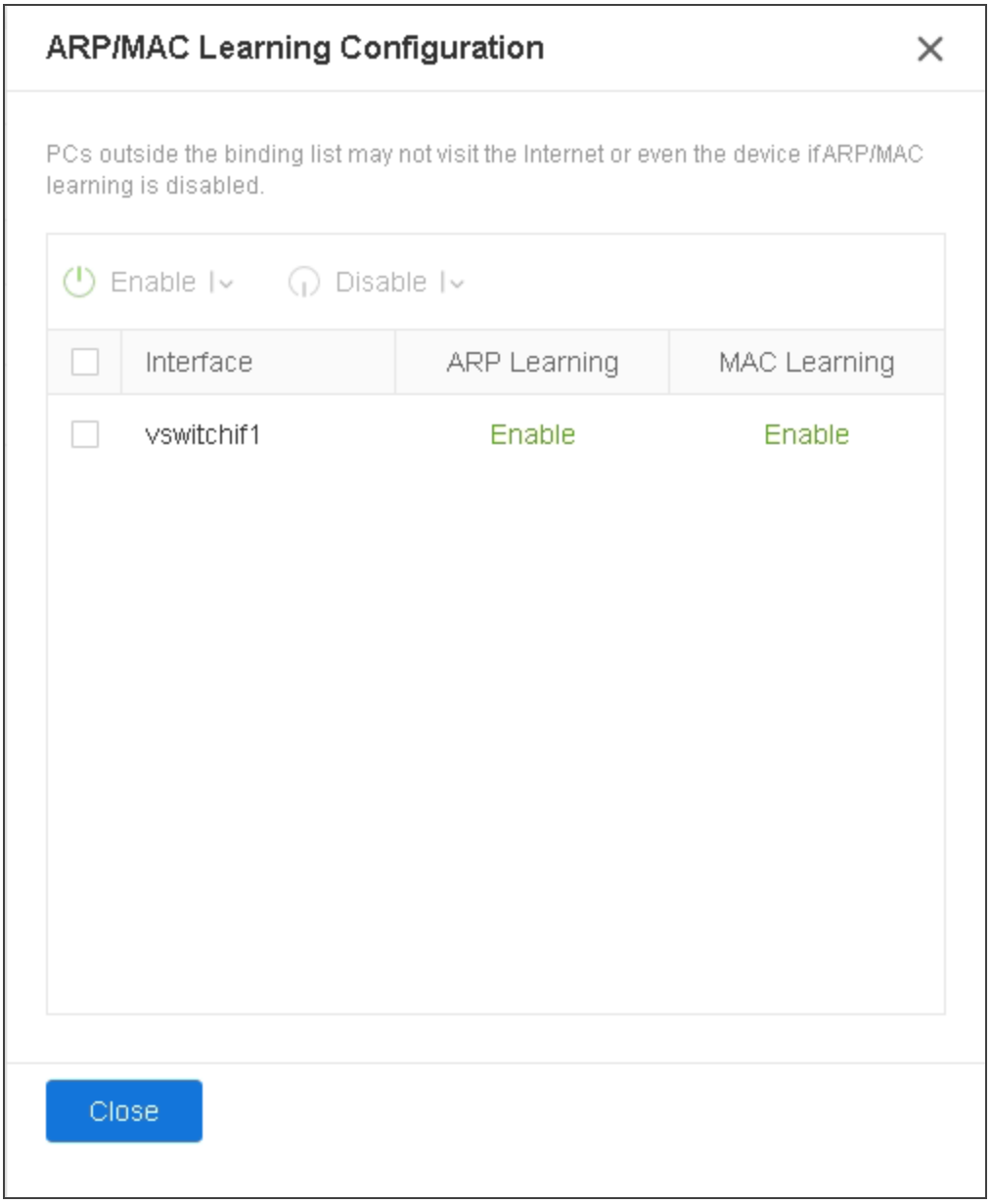
Devices can obtain dynamic IP-MAC-Port binding information from:

- ARP/MAC learning
- IP-MAC scan

To configure the ARP/MAC learning, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.

2. Click ⋮ and click **ARP/MAC Learning** from the pop-up menu.



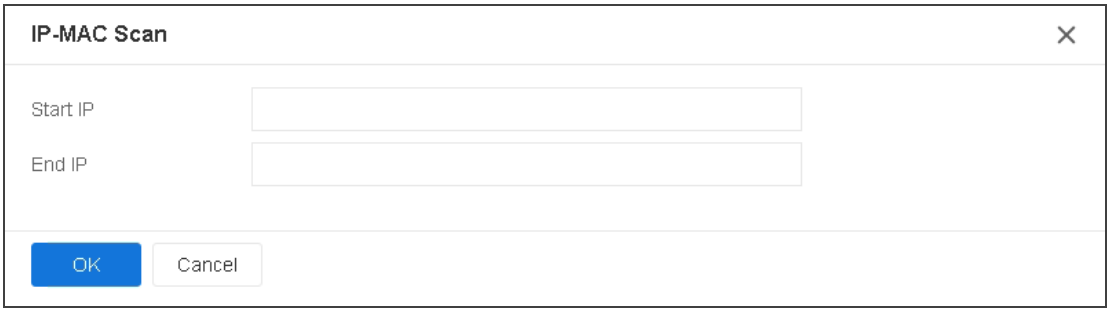
3. In the ARP/MAC Learning Configuration page, select the interface that you want to enable the ARP/MAC learning function.

4. Click **Enable** and then select **ARP Learning** or **MAC Learning** in the pop-up menu. The system will enable the selected function on the interface you select.

5. Close the page and return to the IP-MAC Binding page.

To configure the ARP scan, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select **Binding Configuration** and then click **IP-MAC Scan** from the pop-up menu.



3. In the IP-MAC Scan page, enter the start IP and the end IP.
4. Click **OK** to start scanning the specified IP addresses. The result will display in the table in the IP-MAC binding page.

Viewing the Timeout Period of ARP Entries and MAC Entries

After obtaining the ARP dynamic binding information by using the ARP learning function, ARP scan function, and MAC learning function, you can view the timeout period for ARP and MAC entries from the binding list on the **IP-MAC Binding** page. To refresh the timeout information, you can switch the WebUI pages.



- ARP timeout period: In the **ARP Age (seconds)** column, you can view the timeout of IP-MAC binding in the ARP table. For example, if "1181" is displayed, the IP-MAC binding information will time out 1,181 seconds later. By default, the ARP timeout period of the

interface is 1,200 seconds.

- MAC timeout period: In the **MAC Age (seconds)** column, you can view the timeout of MAC-Port binding in the MAC table. For example, if "586" is displayed, the MAC-Port binding information will time out 227 seconds.

Bind the IP-MAC-Port Binding Item

To bind the IP-MAC-Port binding item, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select **Binding Configuration** and then click **Bind All** from the pop-up menu.
3. In the **Bind All** page, select the binding type.
4. Click **OK** to complete the configurations.

To unbind an IP-MAC-Port binding item:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select **Binding Configuration** and then click **Unbind All** from the pop-up menu.
3. In the **Unbind All** page select the unbinding type.
4. Click **OK** to complete the configurations.

Importing/Exporting Binding Information

To import the binding information, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select ⋮ and then click **Import** from the pop-up menu.
3. In the Import page, click **Browse** to select the file that contains the binding information. Only the UTF-8 encoding file is supported.

To export the binding information, take the following steps:

1. Select **Policy > ARP Defense > IP-MAC Binding**.
2. Select ⋮ and then click **Export** from the pop-up menu.
3. Choose the binding information type.
4. Click **OK** to export the binding information to a file.

Configuring ARP Inspection

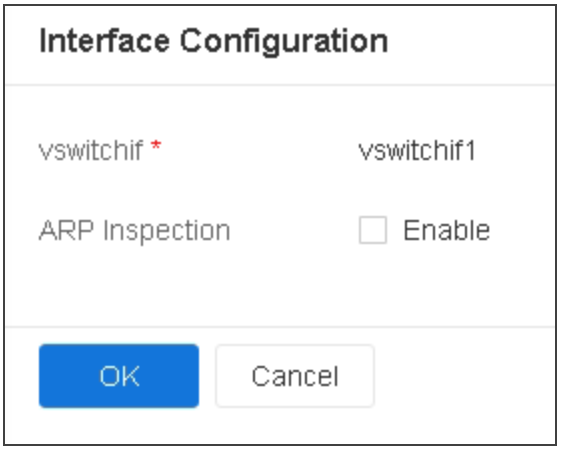
Devices support ARP Inspection for interfaces. With this function enabled, system will inspect all the ARP packets passing through the specified interfaces, and compare the IP addresses of the ARP packets with the static IP-MAC bindings in the ARP list and IP-MAC bindings in the DHCP Snooping list:

- If the IP address is in the ARP list and the MAC address matches, the ARP packet will be forwarded;
- If the IP address is in the ARP list but the MAC address does not match, the ARP packet will be dropped;
- If the IP address is not in the ARP list, continue to check if the IP address is in the DHCP Snooping list;
- If the IP address is in the DHCP Snooping list and the MAC address also matches, the ARP packet will be forwarded;
- If the IP address is in the DHCP Snooping list but the MAC address does not match, the ARP packet will be dropped;
- If the IP address is not in the DHCP Snooping, the ARP packet will be dropped or forwarded according to the specific configuration.

Both the VSwitch and VLAN interface of the system support ARP Inspection. This function is disabled by default.

To configure ARP Inspection of the VSwitch interface, take the following steps:

1. Select **Policy > ARP Defense > ARP Inspection**.
2. System already lists the existing VSwitch interfaces.
3. Double-click the item of a VSwitch interface.

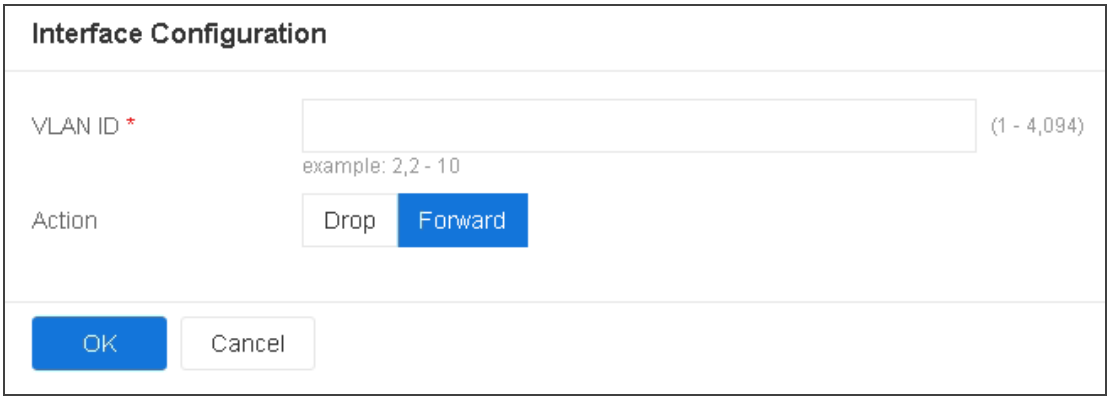


4. In the Interface Configuration page, click the **Enable** button.
5. To drop the traffic whose sender's IP address is not in the ARP table, select **Drop**. To forward the traffic whose sender's IP address is not in the ARP table, select **Forward**.
6. Click **OK** to save the settings and close the page.
7. For the interfaces belonging to the VSwitch interface, you can set the following options:
    - If you do not need the ARP inspection in the interface, in the Advanced Options section, double-click the interface and select **Do Not Inspect** option in the pop-up page.
    - Configure the number of ARP packets received per second. When the ARP packet rate exceeds the specified value, the excessive ARP packets will be dropped. The value range is 0 to 10000. The default value is 0, i.e., no rate limit.

8. Click **OK** to save the settings.

To configure the ARP inspection of the VLAN interface, take the following steps:

1. Select **Policy > ARP Defense > ARP Inspection**.
2. Click **New**.



3. In the Interface Configuration page, specify the VLAN ID.
4. To drop the traffic whose sender's IP address is not in the ARP table, select **Drop**. To forward the traffic whose sender's IP address is not in the ARP table, select **Forward**.
5. Click **OK** to save the settings.

Configuring DHCP Snooping

DHCP, Dynamic Host Configuration Protocol, is designed to allocate appropriate IP addresses and related network parameters for sub networks automatically. DHCP Snooping can create a binding relationship between the MAC address of the DHCP client and the allocated IP address by analyzing the packets between the DHCP client and the server. When ARP Inspection is also enabled, the system will check if an ARP packet passing through can be matched to any binding on the list. If not, the ARP packet will be dropped. In the network that allocates addresses via DHCP, you can prevent against ARP spoofing attacks by enabling ARP inspection and DHCP Snooping.

DHCP clients look for the server by broadcasting, and only accept the network configuration parameters provided by the first reachable server. Therefore, an unauthorized DHCP server in the network might lead to DHCP server spoofing attacks. The devices can prevent DHCP server spoofing attacks by dropping DHCP response packets on related ports.

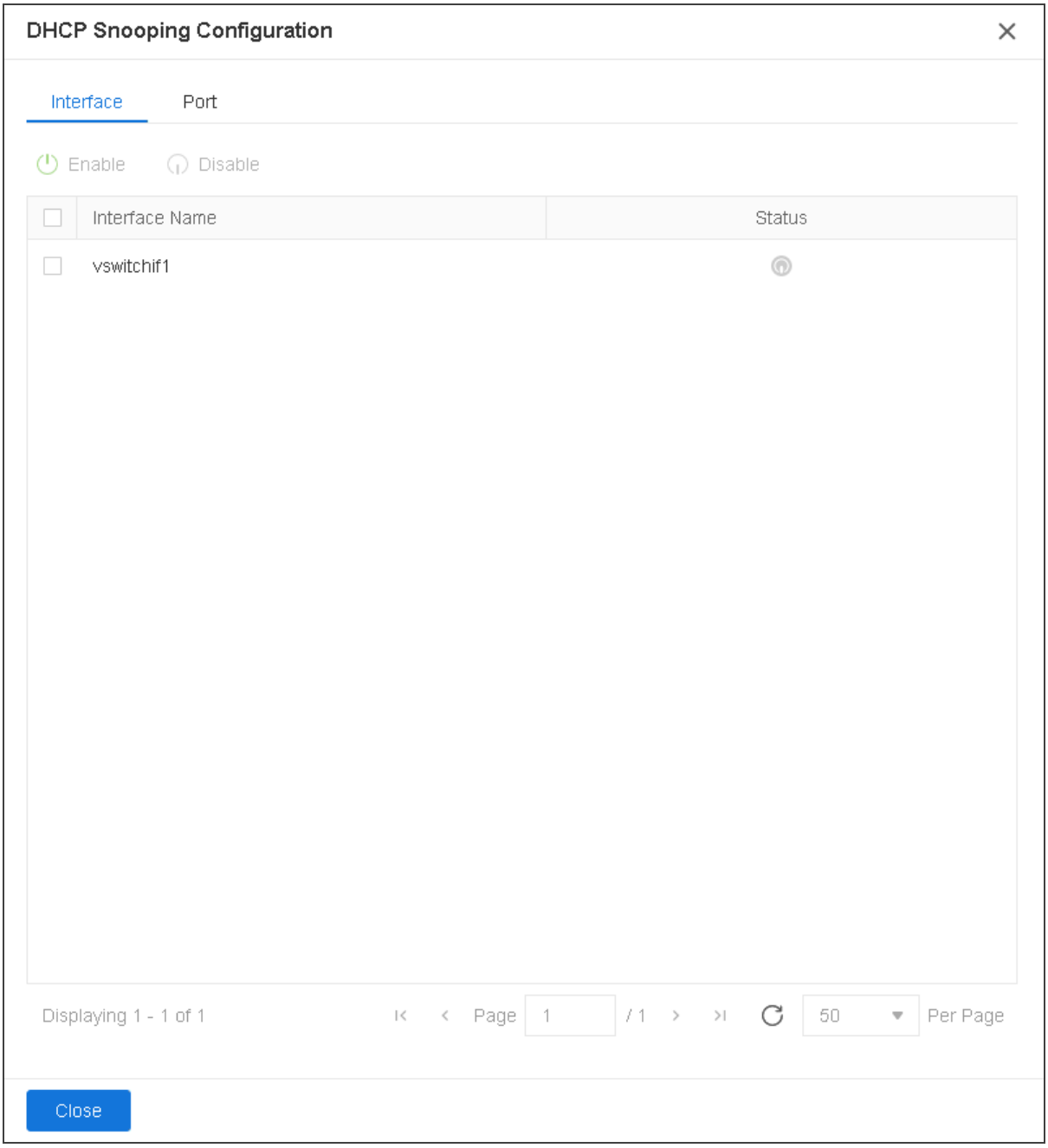
Besides, some malicious attackers send DHCP requests to a DHCP server in succession by forging different MAC addresses, and eventually lead to IP address unavailability to legal users by exhausting all the IP address resources. This kind of attacks is commonly known as DHCP Starvation. The devices can prevent against such attacks by dropping request packets on related ports, setting rate limit or enabling validity check.

The VSwitch interface of the system supports DHCP snooping. This function is disabled by default.

To configure DHCP snooping, take the following steps:

1. Select **Policy > ARP Defense > DHCP Snooping**.

2. Click **DHCP Snooping Configuration**.



3. In the Interface tab, select the interfaces that need the DHCP snooping function.

4. Click **Enable** to enable the DHCP snooping function.

5. In the Port tab, configure the DHCP snooping settings:

    - Validity check: Check if the client's MAC address of the DHCP packet is the same as the source MAC address of the Ethernet packet. If not, the packet will be dropped. Select the interfaces that need the validity check and then click **Enable** to enable this function.

    - Rate limit: Specify the number of DHCP packets received per second on the interface. If the number exceeds the specified value, system will drop the excessive DHCP packets. The value range is 0 to 10000. The default value is 0, i.e., no rate limit. To configure the rate limit, double-click the interface and then specify the value in the **Rate** text box in the pop-up Port Configuration page.

    - Drop: In the Port Configuration page, if the **DHCP Request** check box is selected, the system will drop all of the request packets sent by the client to the server; if the **DHCP Response** check box is selected, system will drop all the response packets returned by the server to the client.

6. Click **OK** to save the settings.

Viewing DHCP Snooping List

With DHCP Snooping enabled, system will inspect all of the DHCP packets passing through the interface, and create and maintain a DHCP Snooping list that contains IP-MAC binding information during the process of inspection. Besides, if the VSwitch, VLAN interface or any other Layer 3 physical interface is configured as a DHCP server, the system will create IP-MAC binding information automatically and add it to the DHCP Snooping list even if DHCP Snooping is not enabled. The bindings in the list contain information like legal users' MAC addresses, IPs, interfaces, ports, lease time, etc.

To view the DHCP snooping list, take the following steps:

1. Select **Policy > ARP Defense > DHCP Snooping**.

2. In the current page, you can view the DHCP snooping list.

Configuring Host Defense

Host Defense is designed to send gratuitous ARP packets for different hosts to protect them against ARP attacks.

To configure host defense, take the following steps:

1. Select **Policy > ARP Defense > Host Defense**.

2. Click **New**.



Sending Settings	
Interface	Specify an interface that sends gratuitous ARP packets.
Excluded Port	Specify an excluded port, i.e., the port that does not send gra-

Sending Settings	
	tuitous ARP packets. Typically it is the port that is connected to the proxied host.
Host	
IP	Specify the IP address of the host that uses the device as a proxy.
MAC	Specify the MAC address of the host that uses the device as a proxy.
Sending Rate	Specify a gratuitous ARP packet that sends rate. The value range is 1 to 10/sec. The default value is 1.

3. Click **OK** to save your settings and return to the Host Defense page.

4. Repeat Step 2 and Step 3 to configure gratuitous ARP packets for more hosts. You can configure the device to send gratuitous ARP packets for up to 16 hosts.

Perimeter Traffic Filtering

Perimeter Traffic Filtering can filter the perimeter traffic based on known risk IP, MAC or Service list, and take logging/block action on the malicious traffic that hits the risk IP, MAC or Service list.

The risk IP list includes the following three types:

- IP Blacklist: The system supports Static IP Blacklist, Blacklist Library, Dynamic IP Blacklist, Real IP Blacklist, and Hit Statistics.
- Service Blacklist: After adding the services to the service blacklist, system will perform the block action to the service until the block duration ends.
- MAC Blacklist: After adding the MAC of the host to the blacklist to prevent users from accessing the network during the specified period.
- IP Reputation list: Retrieve the risk IP (such as Botnet, Spam, Tor nodes, Compromised, Brute-forcer, and so on.) list from the Perimeter Traffic Filtering signature database.
- IP Whitelist: After adding the IP to the IP Whitelist, the system will not block the IP address.
- Global Search: Show the static IP blacklist, blacklist library, dynamic IP blacklist, exception whitelist, service blacklist and IP reputation list entriesof specified IP address .
- Configuration: Blacklist global configuration, including Blacklist Log , Session Rematch and IP Blacklist TCP Reset.



Notes:

- You need to update the IP reputation database before enabling the IP Reputation function for the first time. By default, system will update the database at the certain time everyday, and you can modify the updating settings



according to your own requirements, see "Upgrading System" on Page 1786.

- To upgrade the IP reputation database, install the IP reputation license and reboot. The IP reputation database upgrade function is available only after the device is reboot.

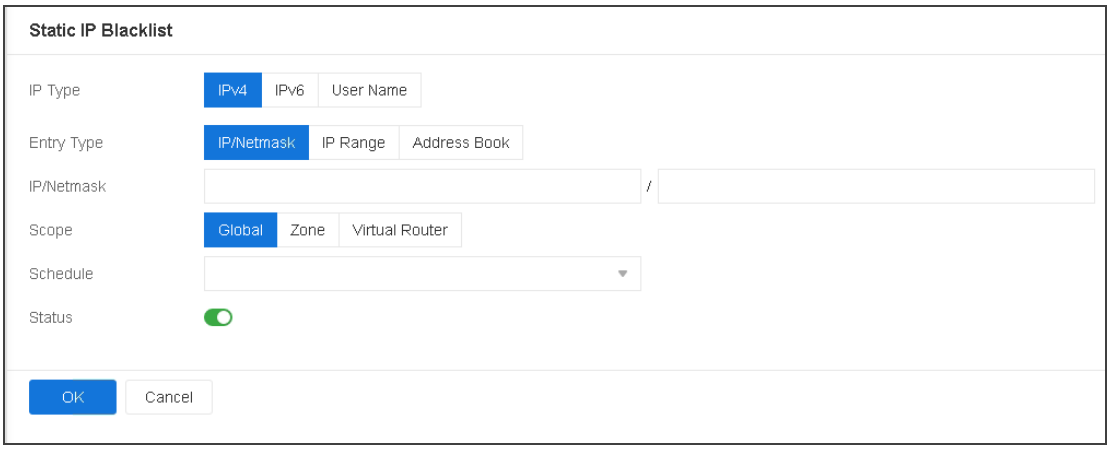
Configuring IP Blacklist

Static IP Blacklist

The static IP blacklist will block specified IP address or prevent hosts from accessing the network during the specified period.

To configure the static IP blacklist, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > IP Blacklist**.
2. Click **New** in the Static IP Blacklist page.



Option	Description
IP Type	Select the address type, including IPv4, IPv6 or User Name. When specified as **User Name**, it means to filter, block or con-

Option	Description
	trol the malicious traffic of the specified user.
Entry Type	Select the address entry type and then type the address.
User Name	When the IP type is specified as "User Name", click the drop-down list to specify the user type and name in the expanded page: • User: Click **AAA Server/Role**, select the AAA server to which the user belongs, and then click the **Select User** drop-down list and select the configured user name or input a user. • User Group: Click **AAA Server/Role**, select the AAA server to which the user group belongs, and then click the **Select User** drop-down list and select the configured user group name or input a user group. • Click **AAA Server/Role**, select the role and search or select the configured role name. **Notes:** Before configuration, please complete the following configuration: create users/user groups and bind IP addresses, create roles and map to users, specify role mapping rules in the AAA server.
Scope	Specify the blacklist applied to global, zone or Virtual Router. When selecting zone or Virtual Router, select the desired entry in the corresponding drop-down list.

Option	Description
Schedule	Specifies a schedule when the blacklist will take effect. Select a desired **schedule** from the Schedule drop-down list.
Status	Specify the status of the static IP blacklist.

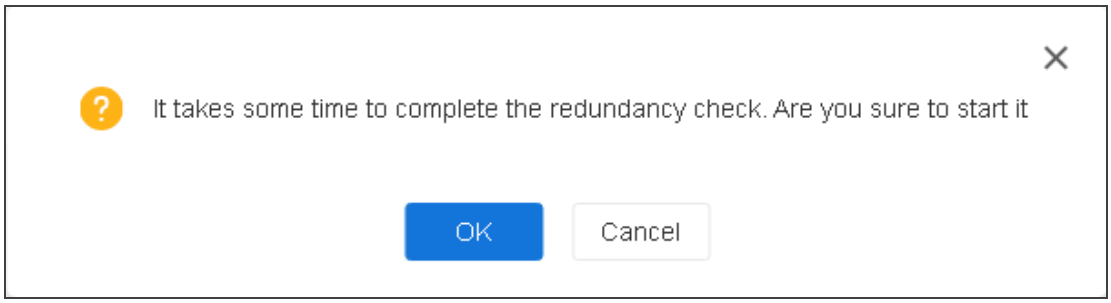
3. Click **OK** to save the settings.

Redundancy Check

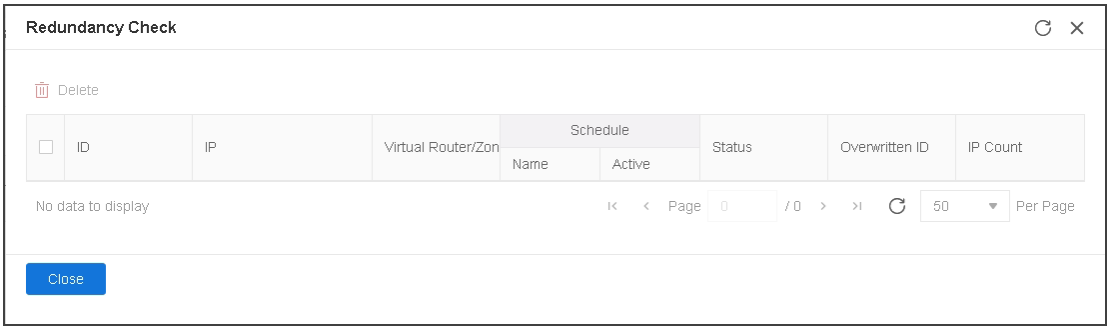
The system supports to check the conflicts among blacklists. You can check whether the blacklists overshadow each other.

To configure the redundancy check, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > IP Blacklist**.
2. Click **Redundancy Check** in the Static IP Blacklist page. Click **OK** in the following prompt dialog.



3. After the check, system will highlight the policy rule which is overshadowed.



4. To delete an blacklist, select the blacklist you want to delete from the list and click **Delete**.

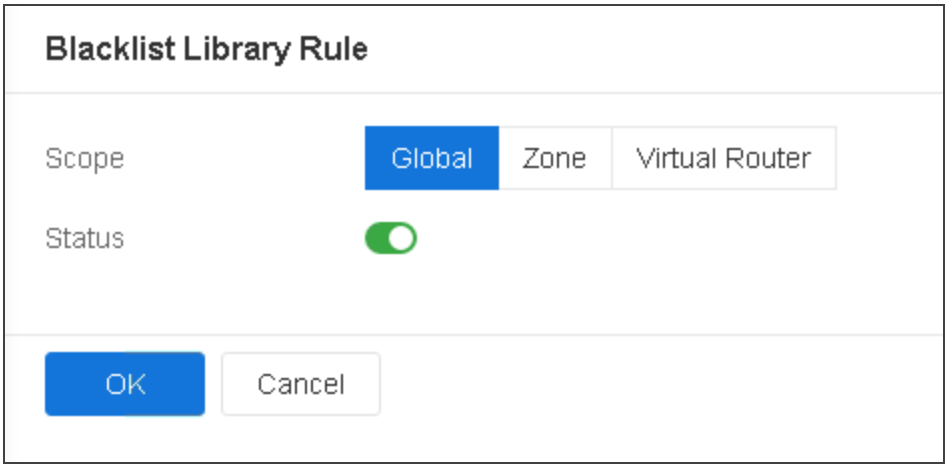
Blacklist Library Rule

The system support to import/export the blacklist library file or update the blacklist from the specified server, and specify the rule of the blacklist library.

To configure the blacklist library rule, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > IP Blacklist**.

2. Click **New** in the Blacklist Library Rule page.



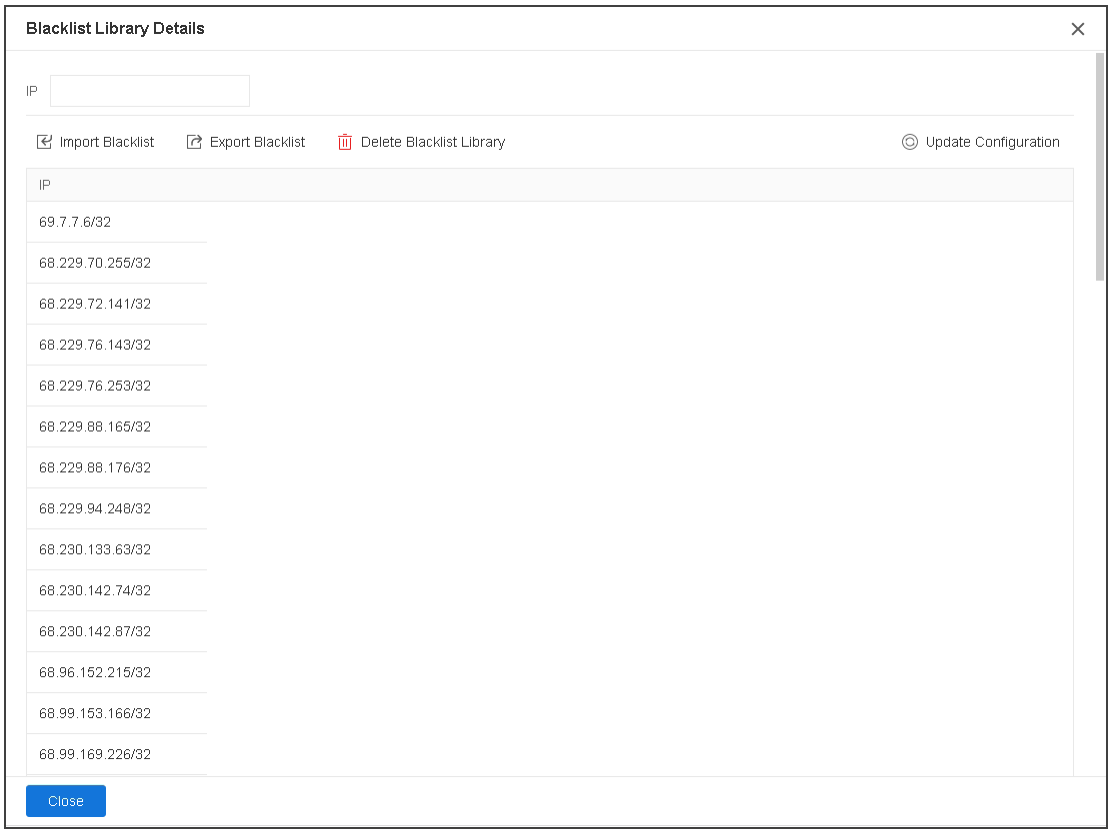
Option	Description
Scope	Specify the blacklist applied to global, zone or Virtual Router.

Option	Description
	When selecting zone or Virtual Router, select the desired entry in the corresponding drop-down list.
Status	Specify the status of the blacklist library rule.

3. Click **OK** to save the settings.

Blacklist Library Details

Click **Blacklist Library Details** to open the Blacklist Library Details page.



To import blacklist library file, take the following steps:

1. Click **Import Blacklist** in the Blacklist Library Details page.
2. Select the import mode, including incremental import and overwrite import.
    - Incremental Import: Import the blacklist library file on the basis of the original file.
    - Overwrite import: Overwrite the original blacklist library file.
3. Click the **Browse** to select the local file to be imported in the File Name area.
4. Click **OK** to save the settings.

To configure auto update, take the following steps:

1. Click **Update Configuration** in the Blacklist Library Details page.
2. Click **Auto Update** to automatically update the blacklist library file from the specified server.

Option	Description
Type	Specifies the time interval for auto update, update at the specified time of every day or the specified time of a specified day during a week.
Server Type	Specifies the server type, including FTP, TFTP, HTTP, and HTTPS.
IP address	If you set the server type to FTP or TFTP, enter the IP address of the server.
URL (Required)	If you set the server type to HTTP or HTTPS, enter the URL of the server in the field. The URL needs to be 1 to 255 characters in length. Note: The URL of the HTTP server needs to start with "http://" and the URL of the HTTPS server needs to start with

Option	Description
	"https://".
Virtual Router (Required)	Specifies the virtual router of the server.
User Name	If you set the server type to FTP, enter the username used to log on to the FTP server.
Password	If you set the server type to FTP, enter the password of the FTP username.
Import Mode	Select the import mode, including incremental import and over-write import.
File Name (Required)	If you set the server type to FTP or TFTP, enter the name of the file to be imported.

3. Click **OK** to save the settings.
4. You can also click **OK And Update Now** to save the settings and update the blacklist library immediately.



Notes:

- The blacklist library file to be imported or automatically updated needs to be in the TXT or CSV format. (This limit applies only to the FTP or TFTP server).
- The size of the blacklist file to be imported or automatically updated cannot be larger than 40 MB.

- The blacklist library files to be imported or automatically updated will be checked for redundancy in the order of import. If the imported entries are completely covered by the first imported entries, the import will be failed.

You can also perform the following operations:

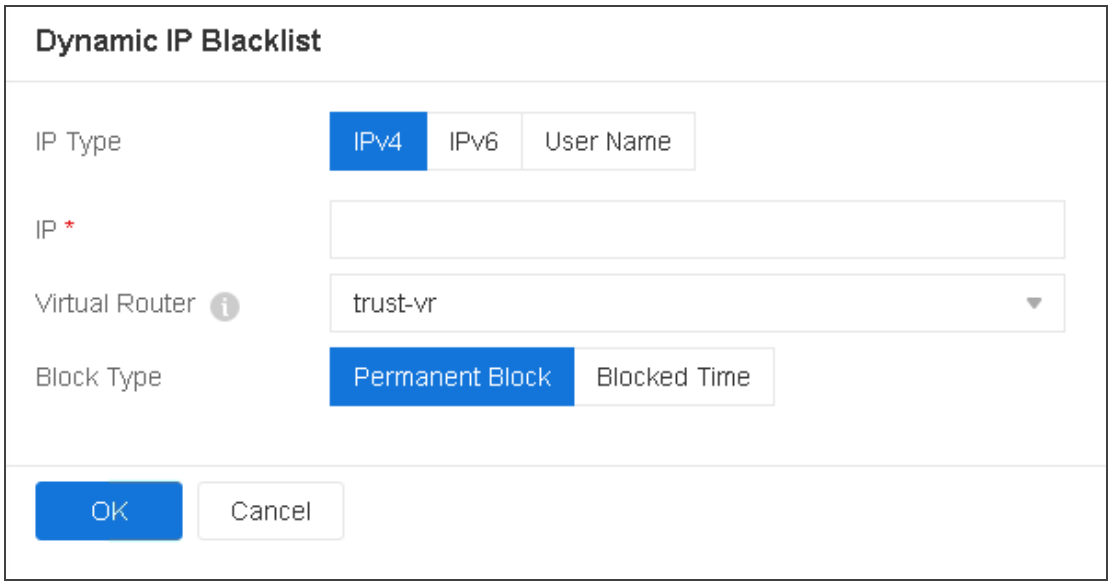
- Export Blacklist: Click **Export Blacklist** to export blacklist file to local PC.
- Delete Blacklist Library: Click **Delete Blacklist Library** to delete the blacklist file.

Dynamic IP Blacklist

After adding the IP addresses to the global blacklist, the system will perform the block action to the IP address and service until the block duration ends.

To configure the dynamic IP blacklist , take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > IP Blacklist**.
2. Click **New** in the Dynamic IP Blacklist tab.



Option	Description
IP Type	Select the address type, including IPv4, IPv6 or User Name. When specified as **User Name**, it means to filter, block or control the malicious traffic of the specified user.
IP	Type the IP address that you want to block. This IP address can be not only the source IP address, but also the destination IP address.
User Name	When the IP type is specified as "User Name", click the drop-down list to specify the user type and name in the expanded page: • User: Click **AAA Server/Role**, select the AAA server to which the user belongs, and then click the **Select User** drop-down list and select the configured user name or input a user. • User Group: Click **AAA Server/Role**, select the AAA server to which the user group belongs, and then click the **Select User** drop-down list and select the configured user group name or input a user group. • Click **AAA Server/Role**, select the role and search or select the configured role name. **Notes:** Before configuration, please complete the following configuration: create users/user groups and bind IP addresses, create roles and map to users, specify role mapping rules in the AAA server.

Option	Description
Virtual Router	Select the virtual router where the blocked IP belongs from the drop-down list.
Block Type	Select the block type, including **Permanent Block** and **Blocked Time**. When **Blocked Time** is selected, type the duration during which the IP address will be blocked. The unit is second. The value ranges from 60 to 1,296,000 seconds.

3. Click **OK**.

Real IP Blacklist

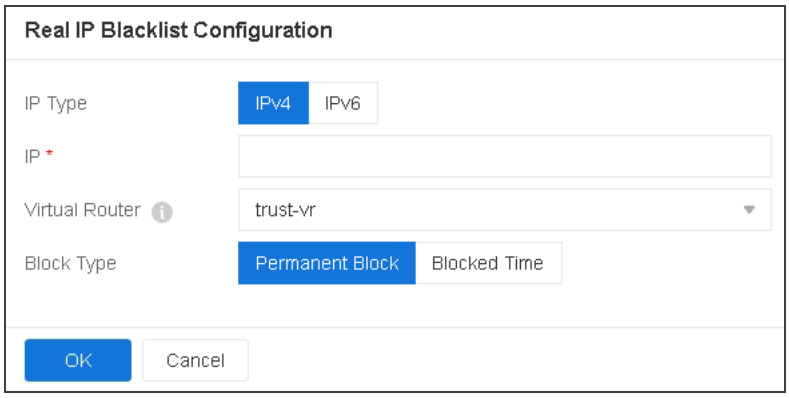
Generally, you can determine the IP address of the client by checking the HTTP packet. However, if the proxy is configured on the client, the source IP contained in the HTTP packet will be the IP address of the proxy server, rather than the real client IP address. In this case, when an attack is detected, the system blocks the IP address of the proxy server, making all services unavailable. To solve this problem, you can determine the real IP address of the client by parsing the X-Forwarded-For and X-Real-IP fields in the HTTP packet. The X-Forwarded-For field is used to record the real IP address of the client and the IP addresses of the proxy servers of different levels. The X-Real-IP field is only used to record the real IP address of the client.

After adding the real IP address of the client to the Real IP Blacklist, the system will perform the block action to that IP address until the block duration ends.

To configure the Real IP Blacklist, take the following steps:

1. Select **Policy** > **Perimeter Traffic Filtering** > **IP Blacklist**

2. Click **New** in the **Real IP Blacklist** tab.



Option	Description
IP Type	Select the IP type, including IPv4 and IPv6.
IP	Type the IP address to be blocked in the text box. This IP address is the real IP address of the client which is parsed by the X-Forwarded-For and X-Real-IP fields in the HTTP packet.
Virtual Router	Select the virtual router where the blocked IP belongs from the drop-down list.
Block Type	Specifies the block type, including **Permanent Block** and **Blocked Time**. **Permanent Block** is the default block type. If **Blocked Time** is selected, type the duration during which the IP address will be blocked. The unit is second. The value ranges from 60 to 1,296,000 seconds.

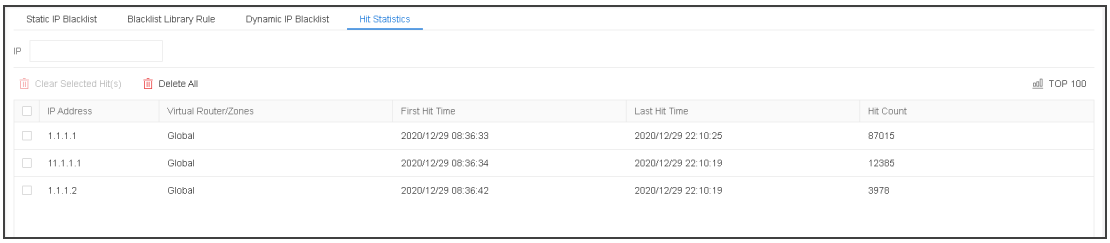
3. Click **OK**.

Hit Statics

System supports statistics on blacklist hit counts, you can view all hit entries and TOP100 black-list entries on the hit statistics page when there is a large number of blacklist entries.

To view a blacklist hit count take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > IP Blacklist**.
2. View all hit entries in the Hit Statics page.



3. Click **TOP 100** to view the TOP 100 hit entries in the Hit Statistics Ranking page.
4. Select the items that need to be cleared, click **Clear Selected Hit(s)** to clear the hit statistics of the specified IP. Click **Delete All** to clear all hit statistics.

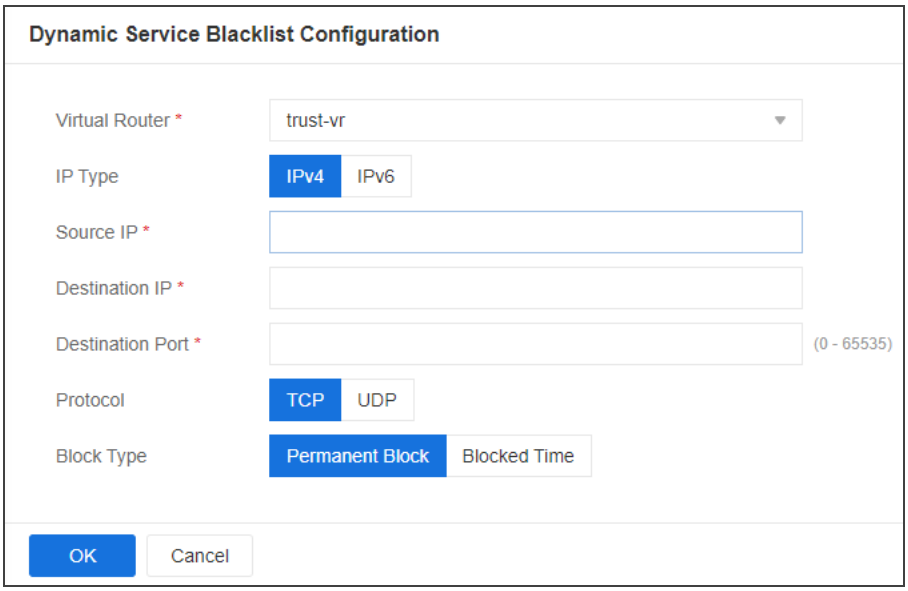
Notes: After deleting the IP blacklist entry, the corresponding hit statistics will also be cleared.

Service Blacklist

To configure the service blacklist, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > Service Blacklist**.

2. Click **New**.



Option	Description
Virtual Router	Select the virtual router that the IP address belongs to.
IP Type	Select the address type, including IPv4 and IPv6.
Source IP	Type the source IP address of the blocked service. The service block function will block the service from the source IP address to the destination IP address.
Destination IP	Type the destination IP address of the blocked service.
Destination Port	Type the port number of the blocked service.
Protocol	Select the protocol of the blocked service.
Blocked Time	Type the duration that the IP address will be blocked. The unit is second. The value ranges from 60 to 1296000.

3. Click **OK** to save the settings.

MAC Blacklist

To configure the MAC blacklist, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > MAC Blacklist**.
2. Click **New**.



Option	Description
MAC address	Type the MAC address of the host that will be added to the blacklist.
Schedule	Specifies a schedule when the blacklist will take effect. Select a desired **schedule** from the Schedule drop-down list.
Status	Specify the status of the MAC blacklist.

3. Click **OK** to save the settings.

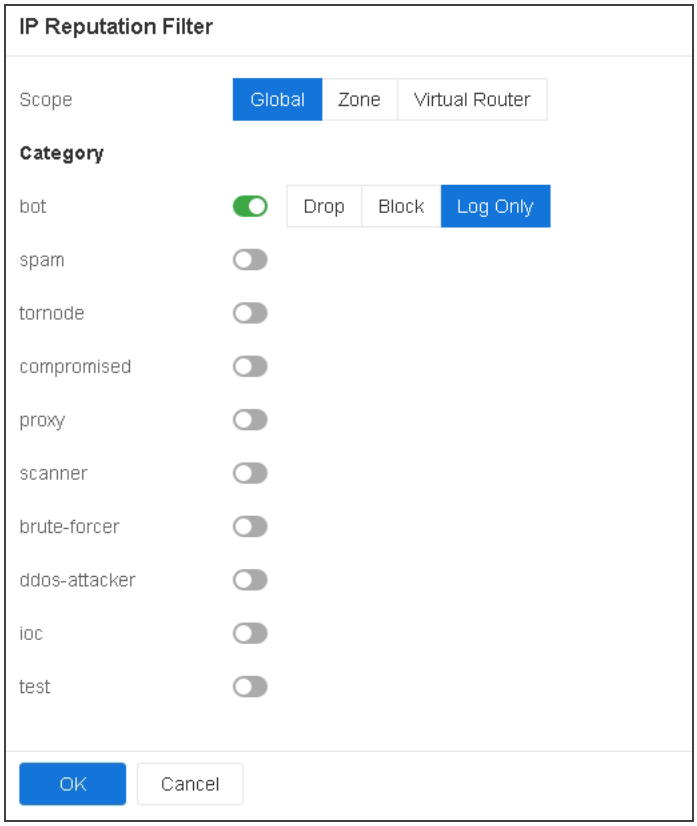
Notes: The configuration of multicast MAC addresses and broadcast MAC addresses is not supported.

IP Reputation Filtering

To configure the IP Reputation Filtering function, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > IP Reputation Filtering**.

2. Click **New**.



Option	Description
Scope	Specify the blacklist applied to global, zone or Virtual Router. When selecting zone or Virtual Router, select the desired entry in the corresponding drop-down list.
Category	Turn on the switch next to a category to enable the IP Reputation Filtering function of the corresponding category. Then, specify the action for the malicious traffic that hits the IP repu-

Option	Description
	tation category. Valid values: Drop, Block, and Log Only (default value). The categories include bot, spam, tornode, compromised, proxy, scanner, brute-forcer, ddos-attacker, and ioc (this category is applicable to the IP blacklist in attack and defense drills).

3. Click **OK** to save the settings.

Configuring IP Whitelist

The system supports Global Whitelist and Perimeter Traffic Filtering Whitelist. The Global Whitelist applies to the whole firewall. For the IP addresses on the Global Whitelist, the system bypasses them without performing security checks. The Perimeter Traffic Filtering Whitelist applies to the perimeter traffic filtering function. For the IP addresses on the Perimeter Traffic Filtering Whitelist, the system does not perform perimeter traffic filtering detection. Therefore, it does not block these IPs.



Notes:

- NAT and Traffic Quota functions are not affected by the Global Whitelist.
- After the NAT function is configured, the system performs perimeter traffic filtering detection before and after the NAT translation. if the IP addresses before and after NAT translation are not all added to the Global Whitelist, the traffic may be blocked by the blacklist.
- Some Attack-Defense types of X-Series devices are not affected by the Global Whitelist. These types are: Teardrop、IP Option、IP Fragment、WinNuke、Ping-of-Death、Huge ICMP Packet、UDP Flood，DNS Flood

To configure IP Whitelist, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > IP WhiteList**.
2. Click **New**.

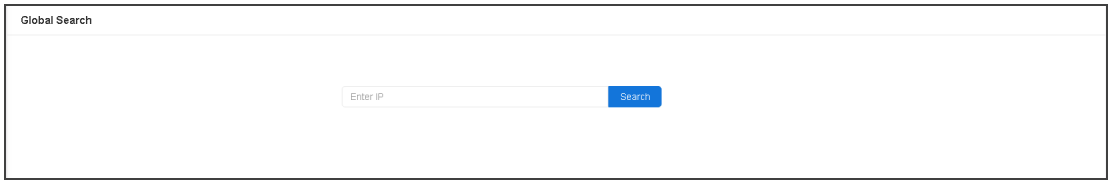
Option	Description
IP Type	Select the address type, including IPv4 and IPv6.
IP/Netmask	Type the IP address and netmask for the user-defined white list.
Global Whitelist	After this function is enabled, the whitelist takes effect globally.
Perimeter Traffic Filtering Whitelist	Specify that the whitelist applys to All Zones, specified Zones or specified Virtual Routers. When "All Zones" is selected, the whitelist takes effect in all security zones or Virtual Routers (that is, in the perimeter traffic filtering module). When selecting "Zone" or "Virtual Router", you must select a security zone or Virtual Router from the drop-down list. Once specified, the whitelist takes effect in the specified security zone or Virtual Router.

3. Click **OK** to save the settings.

Global Search

To view black/white list entry of specified IP address, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > Global Search**.
2. Type the IP address, click **Search** to jump to the corresponding blacklist tab to view the corresponding entry.



Configuration

To configure the blacklist global configuration, take the following steps:

1. Select **Policy > Perimeter Traffic Filtering > Configuration**.
2. Click **Enable** button of Blacklist Log to enable the log of blacklist.
3. Click **Enable** button of Session Rematch. When you add, modify or delete the blacklist, the session will match the optimal blacklist again.
4. Click **Enable** button of IP BlackList TCP Reset. After the IP BlackList TCP Reset is enabled, the system will send a TCP-RST packet to the IP address of TCP traffic that hits the blacklist, thus blocking the IP address.

Chapter 12 Threat Prevention

Threat prevention means that the device that can detect and block network threats. By configuring the threat prevention function, Hillstone devices can defend network attacks and reduce losses of the internal network.

Threat protections include:

- "Anti-Virus" on Page 1302: It can detect the common file types and protocol types which are most likely to carry the virus and protect the network from them. Hillstone devices can detect protocol types of HTTP, FTP, SMTP, POP3 IMAP4 and SMB, and the file types of archives (including GZIP, BZIP2, TAR, ZIP and RAR-compressed archives), PE、HTML、MAIL、RIFF、ELF、PDF、MS OFFICE、Raw Data and Others. **Others** means scans the other file, including GIF, BMP, PNG, JPEG, FWS, CWS, RTF, MPEG, Ogg, MP3, wma, WMV, ASF, RM, etc. If SMB protocol type is used, the system supports the filtering and blocking of virus files in break-point resumption scenarios.
- " Intrusion Prevention System" on Page 1315: It can detect and protect mainstream application layer protocols (DNS, FTP, POP3, SMTP, TELNET, MYSQL, MSSQL, ORACLE, NETBIOS), against web-based attacks and common Trojan attacks.
- "Attack-Defense" on Page 1389: It can detect various types of network attacks, and take appropriate actions to protect the Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.
- "Sandbox" on Page 1376: It can executes suspicious files in the virtual environment, collect dynamic behaviors of suspicious files, analyze these dynamic behaviors, and determine the validity of files based on the analysis results
- "Antispam" on Page 1422: It can filter the mails transmitted by SMTP and POP3 protocol through the cloud server, and discover the mail threats.

- "Botnet Prevention" on Page 1429: It can detect botnet host in the internal network timely, as well as locate and take other actions according to the configuration, so as to avoid further threat attacks.
- "End Point Protection" on Page 1452: It can extract feature data from encrypted traffic and detect the encrypted traffic to check whether threat traffic exists.

The threat protection configurations are based on security zones and policies.

- If a security zone is configured with the threat protection function, system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the threat protection function, system will perform detection on the traffic that is matched to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the threat protection configurations in a destination zone is superior to that in a source zone if specified at the same time.



Notes:

- Threat protection is controlled by a license. To use Threat protection, apply and install the Threat Protection（TP） license, Intrusion Prevention System（IPS）license.

Threat Protection Signature Database

The threat protection signature database includes a variety of virus signatures, Intrusion prevention signatures, Perimeter traffic filtering signatures, . By default system updates the threat protection signature database everyday automatically. You can change the update configuration as needed. Hillstone devices provide two default update servers: https://update1.hillstonenet.com

and https://update2.hillstonenet.com. Hillstone devices support auto updates and local updates. Non-root VSYS does not support updating signature database.

According to the severity, signatures can be divided into three security levels: critical, warning and informational. Each level is described as follows:

- Critical: Critical attacking events, such as buffer overflows.
- Warning: Aggressive events, such as over-long URLs.
- Informational: General events, such as login failures.

Anti-Virus

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The system is designed with an Anti-Virus that is controlled by licenses to provide an AV solution featuring high speed, high performance and low delay. With this function configured in StoneOS, Hillstone devices can detect various threats including worms, Trojans, malware, malicious websites, etc., and proceed with the configured actions.

Anti-Virus function can detect the common file types and protocol types which are most likely to carry the virus and protect the network from them. Hillstone devices can detect protocol types of HTTP, FTP, SMTP, POP3 IMAP4 and SMB, and the file types of archives (including GZIP, BZIP2, TAR, ZIP and RAR-compressed archives), PE、HTML、MAIL、RIFF、ELF、PDF、MS OFFICE、Raw Data and Others. **Others** means scans the other file, including GIF, BMP, PNG, JPEG, FWS, CWS, RTF, MPEG, Ogg, MP3, wma, WMV, ASF, RM, etc. If SMB protocol type is used, the system supports the filtering and blocking of virus files in break-point resumption scenarios.

If IPv6 is enabled, Anti-Virus function will detect files and protocols based on IPv6. How to enable IPv6, see StoneOS_CLI_User_Guide_IPv6.

The virus signature database contains over 10 million signatures. By default, this database supports both daily auto update and real-time local update. See "Security Policy" on Page 1089.

Notes: Anti-Virus is controlled by license. To use Anti-Virus , apply and install the Anti-Virus （AV）license.

Configuring Anti-Virus

This chapter includes the following sections:

- Preparation for configuring Anti-Virus function
- Configuring Anti-Virus function
- Configuring Anti-Virus global parameters

Preparing

Before enabling Anti-Virus, make the following preparations:

1. Make sure your system version supports Anti-Virus.
2. Import an Anti-Virus license and reboot. The Anti-Virus will be enabled after the rebooting.



Notes:

- You need to update the Anti-Virus signature database before enabling the function for the first time. To assure a proper connection to the default update server, you need to configure a DNS server for StoneOS before updating.
- After Anti-Virus is enabled, system's max concurrent sessions might decrease. For more information about the maximum concurrent sessions, see "The Maximum Concurrent Sessions" on Page 1847.

Configuring Anti-Virus Function

The Anti-Virus configurations are based on security zones or policies.

- If a security zone is configured with the Anti-Virus function, system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the threat protection function, system will perform detection on the traffic that is matched to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the threat protection configurations in a destination zone is superior to that in a source zone if specified at the same time.

The system also supports binding the anti-virus profile to a ZTNA policy to perform virus detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

To realize the zone-based Anti-Virus, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. In the Zone Configuration page, expand Threat Protection.
3. Enable the threat protection you need and select an Anti-Virus rule from the profile drop-down list below; or you can click ⊕ from the profile drop-down list. To create an Anti-Virus rule, see Configuring_Anti-Virus_Rule.
4. Click **OK** to save the settings.

To realize the zone-based Anti-Virus, take the following steps:

1. Create a security policy rule. For more information, refer to "Security Policy" on Page 1089.
2. In the Policy Configuration page, expand the Protection tab.

3. Click the **Enable** button of **Anti-virus**. Then select an Anti-Virus rule from the Profile drop-down list, or you can click ⊕ from the Profile drop-down list to create an Anti-Virus rule.

   For more information, see Configuring_Anti-Virus_Rule.

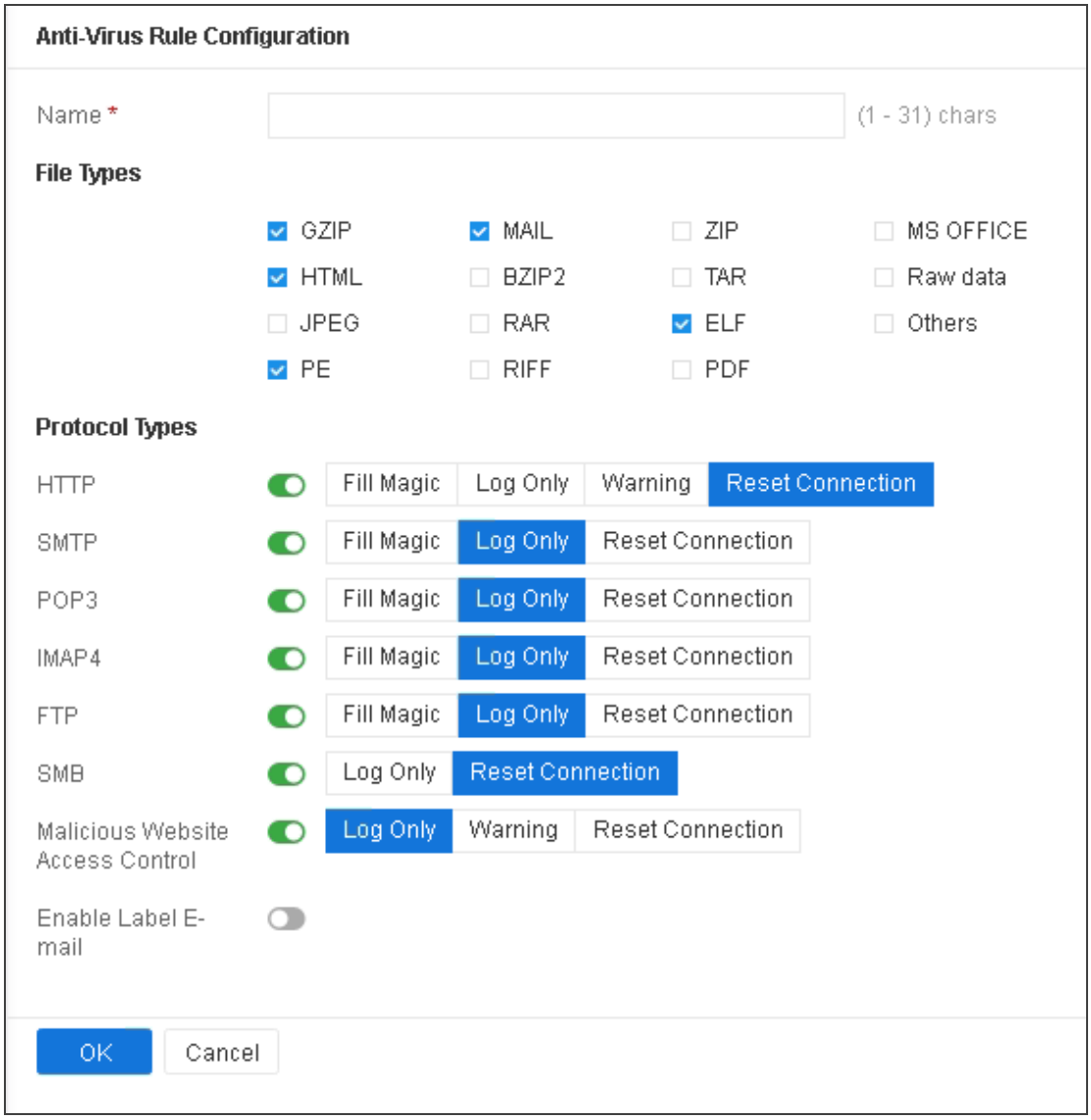
4. Click **OK** to save the settings.

Configuring an Anti-Virus Rule

To configure an Anti-Virus rule, take the following steps:

1. Select **Object > Anti-Virus > Profile**.

2. Click **New**.



Option	Description
Name	Specifies the rule name.
File Types	Specifies the file types you want to scan. It can be GZIP, JPEG, MAIL, RAR, HTML .etc. **Other** means scans the other file, including GIF, BMP, PNG, JPEG, FWS, CWS, RTF, MPEG,

Option	Description
	Ogg, MP3, wma, WMV, ASF, RM, etc.
Protocol Types	Specifies the protocol types (HTTP, SMTP, POP3, IMAP4, FTP,SMB) you want to scan and specifies the action the system will take after the virus is found. • Fill Magic - Processes the virus file by filling magic words, i.e., fills the file with the magic words (Virus is found, cleaned) from the beginning to the ending part of the infected section. • Log Only - Only generates log. • Warning - Pops up a warning page to prompt that a virus has been detected. This option is only effective to the messages transferred over HTTP. • Reset Connection - If virus has been detected, system will reset connections to the files.
Malicious Website Access Control	Click the button behind Malicious Website Access Control to enable the function.
Action	Specifies the action the system will take after the malicious website is found. • Log Only - Only generates log. • Reset Connection - If a malicious website has been detected, system will reset connections to the files.

Option	Description
	• Warning - Pops up a warning page to prompt that a malicious website has been detected. This option is only effective to the messages transferred over HTTP.
Enable Label E-mail	If an email transferred over SMTP is scanned, you can enable label email to scan the email and its attachment(s). The scanning results will be included in the mail body, and sent with the email. If no virus has been detected, the message of "No virus found" will be labeled; otherwise information related to the virus will be displayed in the email, including the filename, result and action. Type the end message content into the box. The range is 1 to 128.

3. Click **OK**.



Notes: By default, according to virus filtering protection level, system comes with three default virus filtering rules: predef_low, predef_middle, predef_high. The default rule is not allowed to edit or delete.

Cloning an Anti-Virus Rule

System supports the rapid clone of an Anti-Virus rule. You can clone and generate a new Anti-Virus rule by modifying some parameters of the one current Anti-Virus rule.

To clone an Anti-Virus rule, take the following steps:

1. Select **Object > Anti-Virus > Profile**.
2. Select an Anti-Virus rule in the list.

3. Click the **Clone** button above the list, and the **Name** configuration box will appear below the button. Then enter the name of the new Anti-Virus rule.

4. The cloned Anti-Virus rule will be generated in the list.

Configuring Anti-Virus Whitelist Function

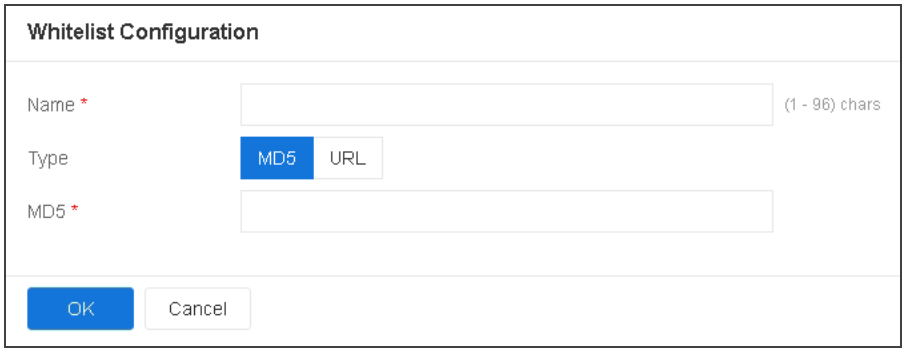
If false positives occur when anti-virus detection is performed on a file or URL, you can add the file MD5 value or URL to an anti-virus whitelist. You can also edit and delete the anti-virus whitelist.

Creating an Anti-Virus Whitelist

To create an anti-virus whitelist, take the following steps:

1. Select **Object** > **Anti-Virus** > **Whitelist**.

2. Click **New**.



Option	Description
Name	Enter the name of the whitelist.
Type	Specifies the whitelist type. Valid values: MD5 and URL.
MD5/URL	Enter the file MD5 value or URL based on the type you specify.

3. Click **OK**.

Notes: At most 1,000 anti-virus whitelists can be added.

Editing an Anti-Virus Whitelist

To edit an anti-virus whitelist, take the following steps:

1. Select **Object** > **Anti-Virus** > **Whitelist**.
2. In the whitelist list, select the whitelist that you want to edit and click **Edit**.
3. On the **Whitelist Configuration** page, edit the whitelist configuration.

Deleting an Anti-Virus Whitelist

To delete an anti-virus whitelist, take the following steps:

1. Select **Object** > **Anti-Virus** > **Whitelist**.
2. In the whitelist list, select the whitelist that you want to delete and click **Delete**.

Configuring Anti-Virus Global Parameters

The Anti-Virus global parameters configuration includes:

- Enabling / Disabling the Anti-Virus function
- Configuring the decompression control function
- Enabling the intelligence file engine detection function

Enabling / Disabling the Anti-Virus function

To enable / disable the Anti-Virus function, take the following steps:

1. Select **Object > Anti-Virus > Configuration**.
2. Click / clear the **Enable** button to enable / disable the Anti-Virus function.
3. In the **Log Aggregate Type**section, select the aggregation type for the anti-virus logs.

- **Do Not Merge**: The system stores each anti-virus log in the database and does not merge any logs.
- **Source IP/Destination IP/Source IP, Destination IP**: Select**Source IP/Destination IP/ Source IP, Destination IP** and specify the **Aggregate Time**. The system merges anti-virus logs of the same merging type based on the specified time granularity, and then stores the merged logs in the database once rather than repeatedly. The number of merged logs is displayed in Attacks Number.
  - **Source IP**: Merges anti-virus logs of the same source IP and MD5.
  - **Destination IP**: Merges anti-virus logs of the same destination IP and MD5.
  - **Source IP, Destination IP**: Merges anti-virus logs of the same source, the same destination IP and MD5.

4. Turn on the switch next to Intelligence File Engine to enable the intelligence file engine detection function. The primary target for detection by the intelligence file engine is PE, PDF, OFFICE, and ELF files. This function can be used to perform malware detection on cached files and delay the transmission of detection messages to ensure successful blocking of virus-infected files. This enhances virus detection and filtering capabilities. By default, this function is disabled. To upgrade the intelligence file engine signature database, see Upgrading Signature Database.
   - Cache File Size: Specify the size of the intelligence file engine cache. Valid values: 128 to 10240 KB. Default value: 1024 KB.
   - Hold Packet Time: Specify the time to delay sending messages. Valid values: 0 to 1000 milliseconds. Default value: 500 milliseconds.
5. Click **OK**.



Notes:

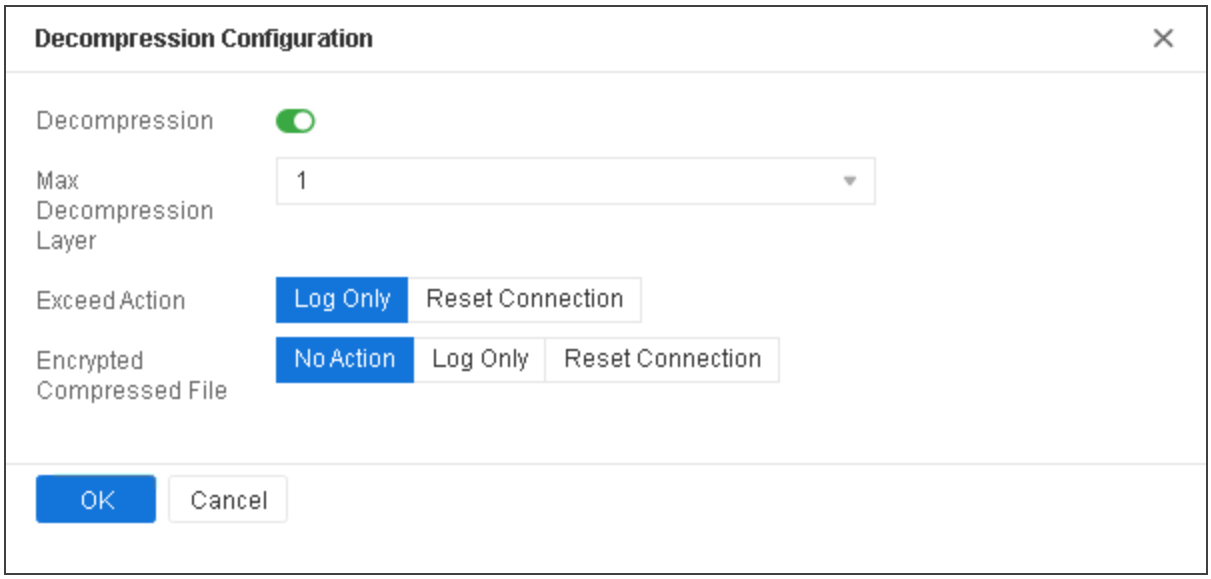
- The configuration to enable/disable the anti-virus function takes effect only after the system is restarted. The configuration of log aggregation takes effect without restarting the system.
- When the action of a protocol in the antivirus profile is set to Fill Magic, files transferred by using this protocol are not detected by the intelligence file engine.
- When the antivirus profile is configured with the Capture Packets action, no packets are captured even if the intelligence file engine detects threats.
- Device except SG-6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800, and SG-6000-A2200 support the intelligence file engine detection function.

Configuring the Decompression Control Function

After configuring the decompression control function, StoneOS can decompress the transmitted compressed files, and can handle the files that exceed the max decompression layer as well as the encrypted compressed files in accordance with the specified actions. This function supports to decompress the files in type of RAR, ZIP, TAR, GZIP, and BZIP2. To configure the decompression control function, take the following steps:

1. Select **Object > Anti-Virus > Configuration**.
2. Click / clear the **Enable** button to enable / disable the Anti-Virus function.

3. Click **Configuration**.



Option	Description
Decompression	Click / clear the **Enable** button to enable / disable the decompression function.
Max Decompression Layer	By default, StoneOS can check the files of up to 5 decompression layers. To specify a decompression layer, select a value from the drop-down list. The value range is 1 to 5.
Exceed Action	Specifies an action for the compressed files that exceed the max decompression layer. Select an action from the drop-down list: • Log Only - Only generates logs but will not scan the files. This action is enabled by default. • Reset Connection - Resets connections for the files.
Encrypted Compressed File	Specifies an action for encrypted compressed files: • No Action - Will not take any actions against the files,

Option	Description
	but might further scan the files according to the Anti-Virus rule. This action is enabled by default. • Log Only - Only generates logs but will not scan the files. • Reset Connection - Resets connections for the files.

4. Click **OK**.



Notes: For compressed files containing docx, pptx, xlsx, jar, and apk formats, when **Exceed Action** is specified as **Reset Connection**, the maximum compression layers should be added one more layer to prevent download failure.

Intrusion Prevention System

IPS, Intrusion Prevention System, is designed to monitor various network attacks in real time and take appropriate actions (like block) against the attacks according to your configuration.

The IPS can implement a complete state-based detection which significantly reduces the false positive rate. Even if the device is enabled with multiple application layer detections, enabling IPS will not cause any noticeable performance degradation. Besides, StoneOS will automatically update the signature database every day by default to assure its integrity and accuracy.

- IPS will support IPv6 address if the IPv6 function is enabled.
- By integrating with the SSL proxy function, IPS can monitor the HTTPS traffic.

The protocol detection procedure of IPS consists of two stages: signature matching and protocol parse.

- Signature matching: IPS abstracts the interested protocol elements of the traffic for signature matching. If the elements are matched to the items in the signature database, system will process the traffic according to the action configuration. This part of detection is configured in the **Select Signature** section.
- Protocol parse: IPS analyzes the protocol part of the traffic. If the analysis results show the protocol part containing abnormal contents, system will process the traffic according to the action configuration. This part of detection is configured in the **Protocol Configuration** section.



Notes: Intrusion Prevention System is controlled by a license. To use Threat protection, apply and install the Intrusion Prevention System (IPS) license.

Signatures

The IPS signatures are categorized by protocols, and identified by a unique signature ID. The signature ID consists of two parts: protocol ID (1st bit or 1st and 2nd bit) and attacking signature

ID (the last 5 bits). For example, in ID 605001, "6" identifies a Telnet protocol, and "05001" is the attacking signature ID. The mappings between IDs and protocols are shown in the table below:

ID	Protocol	ID	Protocol	ID	Protocol	ID	Protocol
1	DNS	7	Other-TCP	13	TFTP	19	NetBIOS
2	FTP	8	Other-UDP	14	SNMP	20	DHCP
3	HTTP	9	IMAP	15	MySQL	21	LDAP
4	POP3	10	Finger	16	MSSQL	22	VoIP
5	SMTP	11	SUNRPC	17	Oracle	-	-
6	Telnet	12	NNTP	18	MSRPC	-	-

In the above table, Other-TCP identifies all the TCP protocols other than the standard TCP protocols listed in the table, and Other-UDP identifies all the UDP protocols other than the standard UDP protocols listed in the table.

Configuring IPS

This chapter includes the following sections:

- Preparation for configuring IPS function
- Configuring IPS function

Preparation

Before enabling IPS, make the following preparations:

1. Make sure your system version supports IPS.
2. Import an Intrusion Prevention System (IPS) license and reboot. The IPS will be enabled after the rebooting.



Notes: After IPS is enabled, system's max concurrent sessions might decrease. For more information about the maximum concurrent sessions, see "The Maximum Concurrent Sessions" on Page 1847.

Configuring IPS Function

The IPS configurations are based on security zones or policies.

- To perform the IPS function on the HTTPS traffic, see the policy-based IPS.

The system also supports binding the IPS profile to a ZTNA policy to perform IPS detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

To realize the zone-based IPS, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. In the Zone Configuration page, expand Threat Protection.

3. Enable the IPS you need and select an IPS rules from the profile drop-down list below, or you can click ⊕ from the profile drop-down list below. To create an IPS rule, see Configuring_an_IPS_Rule.

4. Click a direction (Inbound, Outbound, Bi-direction). The IPS rule will be applied to the traffic that is matched with the specified security zone and direction.

To realize the policy-based IPS, take the following steps:

1. Create a policy rule. For more inform action, refer to "Security Policy" on Page 1089.

2. In the Policy Configuration page, expand Protection.

3. Click the **Enable** button of **IPS**. Then select an IPS rule from the Profile drop-down list, or you can click ⊕ from the Profile drop-down list to create an IPS rule. For more information, see Configuring_an_IPS_Rule.

4. To perform the IPS function on the HTTPS traffic, you need to enable the SSL proxy function for the above specified security policy rule. System will decrypt the HTTPS traffic according to the SSL proxy profile and then perform the IPS function on the decrypted traffic.

   According to the various configurations of the security policy rule, system will perform the following actions:

Policy Rule Configurations	Actions
SSL proxy enabled IPS disabled	System decrypts the HTTPS traffic according to the SSL proxy profile but it does not perform the IPS function on the decrypted traffic.
SSL proxy	System decrypts the HTTPS traffic according to the SSL proxy

Policy Rule Configurations	Actions
enabledIPS enabled	profile and performs the IPS function on the decrypted traffic.
SSL proxy disabled IPS enabled	System performs the IPS function on the HTTP traffic according to the IPS profile. The HTTPS traffic will not be decrypted and system will transfer it.

If the destination zone or the source zone specified in the security policy rule is configured with IPS as well, system will perform the following actions:

Policy Rule Configurations	Zone Configurations	Actions
SSL proxy enabled IPS disabled	IPS enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS function on the decrypted traffic according to the IPS rule of the zone.
SSL proxy enabled IPS enabled	IPS enabled	System decrypts the HTTPS traffic according to the SSL proxy profile and performs the IPS function on the decrypted traffic according to the IPS rule of the policy rule.
SSL proxy disabled IPS enabled	IPS enabled	System performs the IPS function on the HTTP traffic according to the IPS rule of the policy rule. The HTTPS traffic will not be decrypted and system will transfer it.

5. Click **OK** to save the settings.

Configuring an IPS Rule

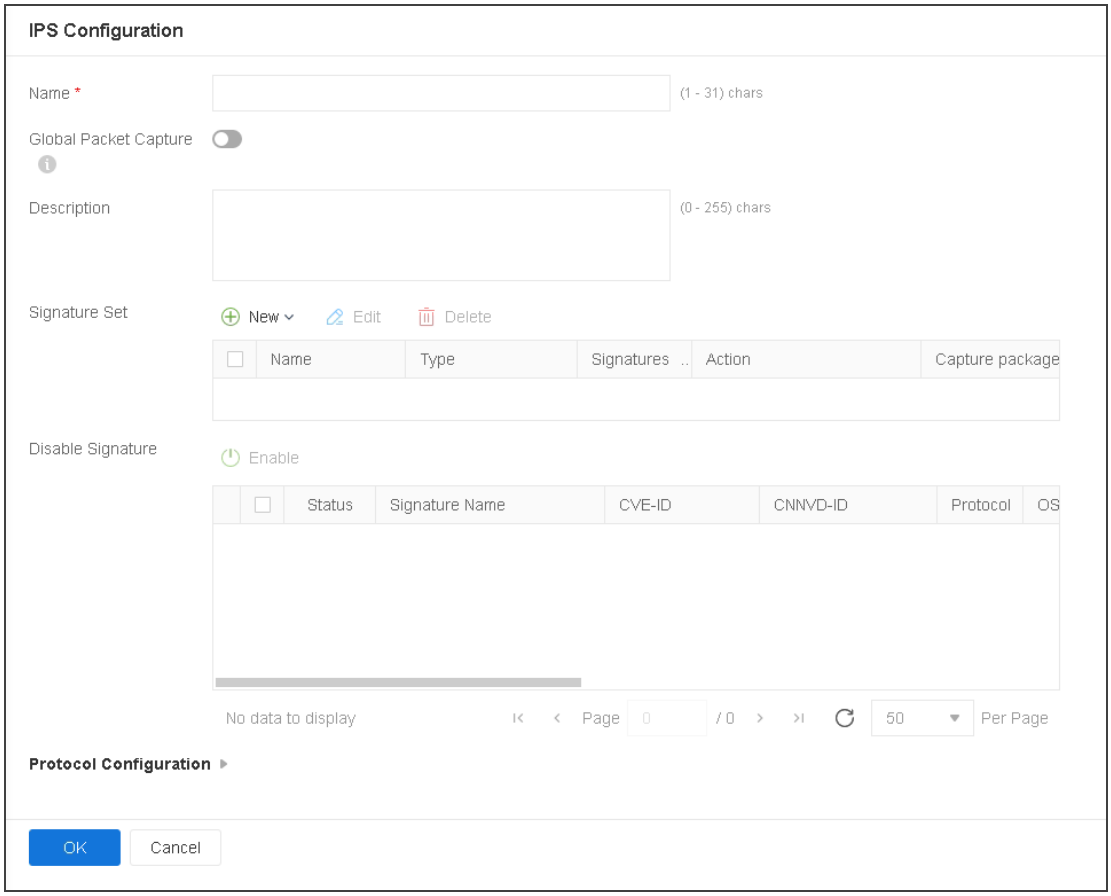
System has three default IPS rules: **predef_default** , **predef_loose** and **predef_critical**.

- The **predef_default** rule is configured with IPS signatures of medium and high confidence levels, this rule can be used to detect threats and perform the default rule action.
- The **predef_loose** rule is configured with all the IPS signatures and its default action is log only.
- The **predef_critical** rule is configured with IPS signatures of the latest high-risk attacks and its default action is reset.

The system supports up to 64 user-defined IPS rules and each non-root VSYS supports up to 4 user-defined IPS rules.

To configure an IPS rule, take the following steps:

1. Select **Object > Intrusion Prevention System > Profile**.
2. Click **New** to create a new IPS rule. To edit an existing one, select the check box of this rule and then click **Edit**. To view it, click the name of this rule.



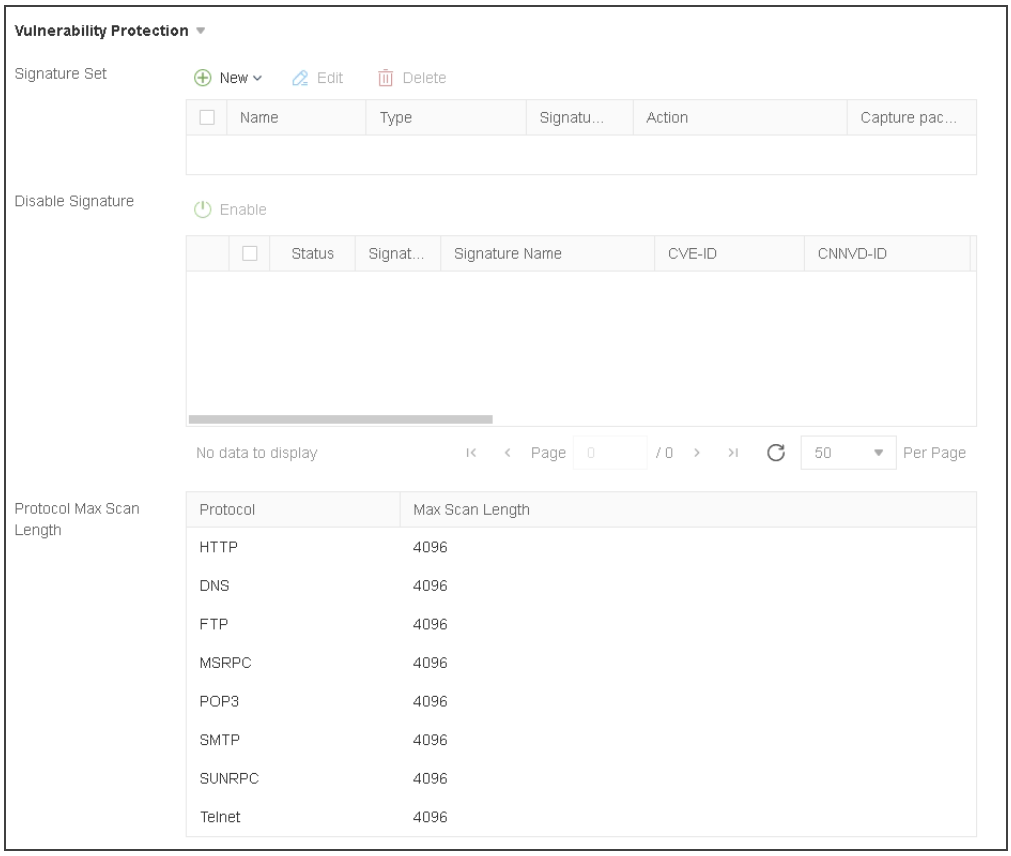
Note: A navigation bar is located on the right side of the **IPS Configuration** page. You can click any option to go to the corresponding section.

3. Configure the basic information of the profile:

Option	Description
Name	In the Name text box, enter the name of the newly-created IPS IDS profile. If you just configure the name and click **OK**, this profile will not take effect.
Global Packet Capture	Click the **Enable** button of Global Packet Capture to capture packets.

Option	Description
Description	Type the description information into the **Description** text box.

4. In the **Vulnerability Protection** section, click ▸ next to Vulnerability Protection to expand this section, including **Signature Set** and **Protocol Max Scan Length**.



5. In the signature configuration area, configure signature set rules and disable signatures.

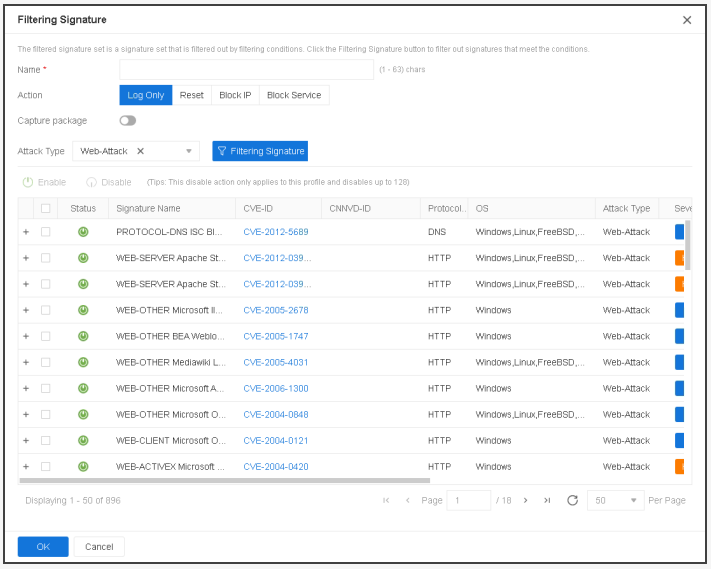
    i. In the **Signature Set** area, the existing signature sets and their settings will be displayed in the table. Select the desired signature sets. You can also manage the signature sets, including **New**, **Edit**, and **Delete**. When creating a new signature set rule, you can select **Filtering Signature** or **Selection Signature** as needed to filter and retrieve the signature database to select the desired signature sets.

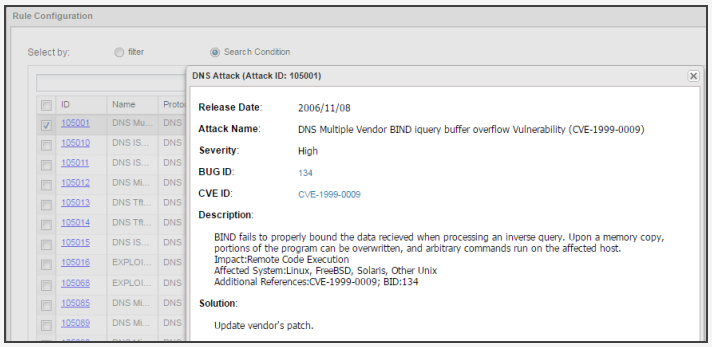
- Filtering Signature: Filter signature sets by certain filter conditions. Click the **Filter Signature** button to search for the signatures you want. In this way, you can quickly select the signatures that have been classified by system.
- Selection Signature: Select a particular signature set from the signature database. In this way, you can quickly select a particular signature.

ii. **Click New and select Filtering Signature or Selection Signature to create a new signature set rule.**

Option	Description
Name	Specify the name of signature.
Action	Specify the action performed on the abnormal traffic that matches the signature set. • Log Only: Record a log. • Reset: Reset connections (TCP) or send destination unreachable packets (UDP) and also generate logs. • Block IP: Block the IP address of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker. • Block Service: Block the service of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify

Option	Description
	a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. • Default: Excute the action specifiled in the signature rule.
Capture Packet	Capture the abnormal packets that match the configured signature set. You can view and download them in the threat log.
Filtering Signature	If **Filtering Signature** is selected: System categorizes the signatures according to the following aspects (aka main categories): affected OS, attack type, protocol, severity, confidence, released year, affected application, and bulletin board. A signature can be in several subcategories of one main category. For example, the signature of ID 200211 is in the Linux subcategory, the FreeBSD subcategory, and Other Linux subcategory at the same time. Note: By default, **Filtering Signature** filters signatures based on all subcategories of severity. You can select other dimensions for filtering. You can view the detailed information of the signature by clicking the signature ID, and you can select one or more signatures. Click the Disable or Enable button to disable or re-enable the signature. **Note**: The enabled/disabled state here is only for the current profile, but the global state is not affected.

Option	Description
	 When selecting main category and subcategory, note the following matters: • You can select multiple subcategories of one main category. The logic relation between them is OR. • The logic relation between each main category is AND. • For example, you have selected Windows and Linux in OS and select HIGH in Severity. The chosen signatures are those whose severity is high and meanwhile whose affected operating system is either Windows or Linux.
Selection Signature	If **Selection Signature** is selected: Type the signature information into the **Keyword** text box, and system will perform fuzzy search in the following fields: signature ID,

Option	Description
	signature name, and description.  After the matched signature is found, select the signature, and it will be added to the Selected Signatures tab, indicating the signature is included in the signature set. After the matched signature is found, select the signature, and then click the Enable or Disable button to disable or re-enable the signature. The enabled/disabled state here is only for the current profile, but the global state is not affected.
Note: You create several signature sets and some of them contain a particular signature. If the actions of these signature sets are different and the attack matches this particular signature , system will adopt the following rules: • Always perform the stricter action on the attack. The signature set with stricter action will be matched. The strict level is: Block IP > Block Service > Rest > Log Only > Deault. If one signature set is Block IP with 15s and the other is Block Service with 30s, the final action will be Block IP with 30s.	

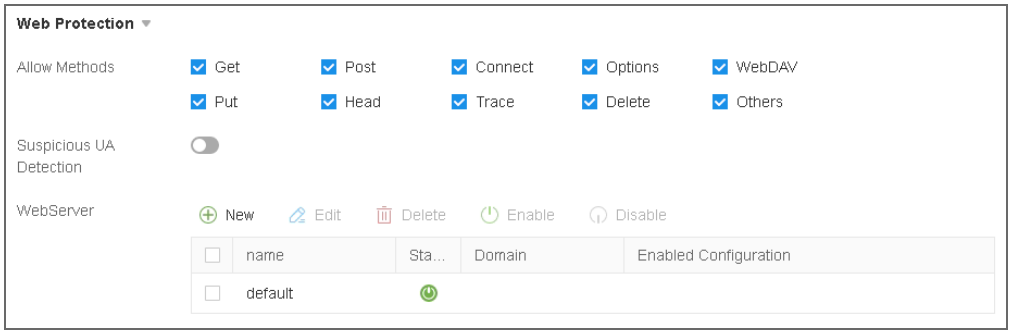
Option	Description
	• If one signature set is configured with Capture Packet, system will capture the packets. • The action of the signature set created by Selection Signature has higher priority than the action of the signature set created by Filter.

iii. Click **OK** to complete signature set configurations.

iv. In the Disable Signature section, the signatures that are Disabled in the template will be shown. Select one or more signatures, and then click the **Enable** button to re-enable the signature.

6. In the **Protocol Max Scan Length** section of **Vulnerability Protection**, click the max scan length of any protocol in the table to modify it. You can configure the max scan length of the HTTP, DNS, FTP, MSRPC, POP3, SMTP, SUNRPC, and Telnet protocols. Default max scan length: 4096 bytes. Valid values: 0 to 65535 bytes, in which 0 indicates no limits.

7. **In the Web Protection section, click ▸ next to Web Protection to expand this section.**



Option	Description
Allow Methods	Specify the HTTP method that is allowed, including Get, Post, Connet, Options, WebDAV, Put, Head, Trace, Delete, and Others.

Option	Description
Suspicious UA Detection	Turn on the switch to enable the Suspicious UA Detection function. With this function enabled, the system detects User-Agent in HTTP Request messages. When User-Agent is detected as abnormal in HTTP messages, you can specify the action to handle User-Agent.

	Action: Specify the action to be performed when suspicious UA is detected.
	• Log Only: Record a log.
	• Block IP: Block the IP address of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service: Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "per-

Option	Description
	manent" to permanently block the service of the attacker.

To protect the Web server, configure Web Server in the HTTP tab.

Protecting the Web server means system can detect the following attacks: Sensitive File Scan, High Frequency Access Control, SQL injection, XSS injection, external link check, hotlinking check, iframe attack, ACL, and HTTP request flood and take actions when detecting them.

A pre-defined Web server protection rule named **default** is built in. The **default** rule supports only the following protection functions: Sensitive File Scan, SQL injection protection, XSS injection detection, iframe check, ACL, and HTTP request flood protection. By default, this protection rule is enabled and cannot be disabled or deleted. Each IPS rule can configure at most 32 Web server protection rules, excluding the **default** rule.

Configure the following settings to protect the Web server:

Option	Description
Name	Specify the name of the Web server protection rule.
Configure Domain	Specify domains protected by this rule. Click the link and the Configure Domain page will appear. Enter the domain names in the **Domain** text box. At most 5 domains can be configured. The traffic to these domains will be checked by the protection rule. The domain name of the Web server follows the longest match rule from the back to the front. The traffic that does not match any rules will match the default Web server. For example, you have configured two protection rules: **rule1 and rule2**. The

Option	Description
	domain name in rule1 is abc.com. The domain name in rule2 is email.abc.com. The traffic that visits news.abc.com will match rule1, the traffic that visits www.email.abc.com will match rule2, and the traffic that visits www.abc.com.cn will match the default protection rule.
High Frequency Access Control	Click the Enable button to enable the High Frequency Access Control feature. When this function is enabled, system will block the traffic of this IP address, whose access frequency exceeds the threshold. • Threshold: Specifies the maximum number of times a single source IP accesses the URL path per minute. When the frequency of a source IP address exceeds this threshold, system will block the flow of the IP. The value ranges from 1 to 65535 times per minute. • URL Path: Click the link and the URL Page Configuration page appears. Click **New** and enter the URL path in the **Path** text box. After the configuration, all paths that contain the name of the path are also counted. System accesses the frequency statistics for HTTP requests that access these paths. If the access frequency of the HTTP request exceeds the threshold, the source IP of the request is blocked, and the IP will not be able to access the Web server. For example: configure'/home/ab', sys-

Option	Description
	tem will perform a frequency check on the 'access/home/-ab/login' and '/home/BC/login' HTTP requests. URL path does not support the path format which contains the host name or domain name, for example: you can not configure www.baidu.com/home/login.html, you should configure '/ home / login.html', and 'www.baidu.com' should be configured in the corresponding Web server domain name settings. You can configure up to 32 URL paths. The length of each path is in the range of 1-255 characters. **Note**: Non-root VSYS does not support the High Frequency Access Control.
Sensitive File Scan	Select Enable to enable the Sensitive File Scan function for Web servers. In Sensitive File Scan attacks, an attacker traverses the sites in the Web server by using a file scanning tool. This way, the attacker can obtain sensitive information of the Web server, such as the directory structure, background files, and backup files. If an attacker attempts to scan sensitive files on the Web server, the Web server returns a large number of response packets with the status code "404". In this case, the system counts the number of 404 responses returned by the Web server per minute. ① If the number is greater than 10, the system parses the URLs in

Option	Description

	all HTTP requests and matches them with the built-in sensitive file dictionary. If the number of times that the parsed URL matches the sensitive file dictionary exceeds the specified threshold, the system performs the user-specified protection actions. The specified actions can be Log Only, Reset, Block IP, or Block Service. ②If the number is equal to or greater than 100, the system determines the behavior as a sensitive file scanning attack and performs the specified protection action.
	• Threshold: Specifies the threshold for the system to defend against sensitive file scanning attacks. If the number of times that URL paths match sensitive file dictionaries per minute exceeds the threshold, the system performs the user-specified protection actions. Default value: 10. Valid values: 10 to 100. Unit: times/min.
	• Action: Specifies the protection action for the system to defend against sensitive file scanning attacks: Log Only, Block IP, or Block Service.
	  • Log Only: record a log.
	  • Reset: Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
	  • Block IP: Block the IP address of the attacker and

Option	Description
	specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the attacker's IP address of the attacker. • Block Service: Block the service of the attacker and specify a block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
SQL Injection Protection	Click the Enable button to enable SQL injection check. • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. • Check point: Specifies the check point for the SQL injec-

Option	Description
	tion check. It can be Cookie, Cookie2, Post, Referer or URI.
XSS Injection Protection	Click the Enable button box to enable XSS injection check for the HTTP protocol. • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs. Block IP - Block the IP address of the attacker and specify a block duration. Block Service - Block the service of the attacker and specify a block duration. • Check point: Specifies the check point for the XSS injection check. It can be Cookie, Cookie2, Post, Referer or URI.
External Link Check	Click the Enable button to enable external link check for the Web server. This function controls the resource reference from the external sites. • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • External link exception: Click this link, and the External Link Exception Configuration page will appear. All the

Option	Description
	URLs configured on this page can be linked by the Web sever. At most 32 URLs can be specified for one Web server. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
Hotlinking Check	Click the Enable button to enable Hotlinking Check. System checks the headers of the HTTP packets and obtains the source site of the HTTP request. If the source site is in the Hotlinking Exception list, system will release it; otherwise, log or reset the connection. Thus controlling the Web site from other sites and to prevent chain of CSRF (Cross Site Request Forgery cross-site request spoofing) attacks occur. • Hotlinking Exception: Click the 'Hotlinking Exception ' to open the <Hotlinking Exception Configuration> page, where the configured URL can refer to the other Web site. Each Web server can be configured with up to 32 URLs. • Action: Specify the action for the HTTP request for the chaining behavior, either "Log only" or "Reset". “
Iframe check	Click the Enable button to enable iframe checking. System will identify if there are hidden iframe HTML pages by this function, then log it or reset its link.

Option	Description
	After iframe checking is enabled, system checks the iframe in the HTML page based on the specified iframe height and width, and when any height and width is less than or equal to the qualified value, system will identify as a hidden iframe attack, record, or reset connection that occurred. • Height: Specifies the height value for the iframe, range from 0 to 4096. • Width: Specifies the width value of the iframe, range from 0 to 4096. • Action: Specify the action for the HTTP request that hides iframe behavior, which is 'Only logged' or 'Reset'. Log Only - Record a log. Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
ACL	Click the Enable button to enable access control for the Web server. The access control function checks the upload paths of the websites to prevent the malicious code uploading from attackers. • ACL: Click this link, the ACL Configuration page appears. Specify websites and the properties on this page. "Static" means the URI can be accessed statically only as the static resource (images and text), otherwise, the access will handle as the action specified (log only/reset); "Block"

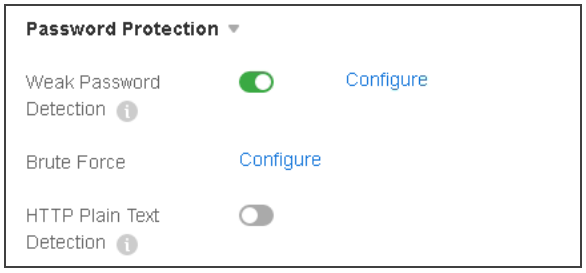
Option	Description
	means the resource of the website is not allowed to access. • Action: Log Only - Record a log. Rest - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs.
HTTP Request Flood Protection	Select the Enable check box to enable the HTTP request flood protection. Both IPv4 and IPv6 address are supported. • Request threshold: Specifies the request threshold. For the protected domain name, when the number of HTTP connecting request per second reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack, and will enable the HTTP request flood protection. • When the number of HTTP connecting request per second by the object reaches the threshold and this lasts 20 seconds, system will treat it as a HTTP request flood attack by this object, and will enable the HTTP request flood protection. • x-forwarded-for: Select None, system will not use the value in x-forwarded-for as the statistic object. Select First, system will use the first value of the x-forwarded-for field as the statistic object. Select Last, system will use the last value of the x-for-

Option	Description
	warded-for field as the statistic object. Select All, system will use all values in x-forwarded-for as the statistic object. • x-real-ip: Select whether to use the value in the x-real-ip field as the statistic field. When the HTTP request flood attack is discovered, you can make the system take the following actions: • Authentication: Specifies the authentication method. System judges the legality of the HTTP request on the source IP through the authentication. If a source IP fails on the authentication, the current request from the source IP will be blocked. The available authentication methods are: • No Authentication: The system does not authenticate the source IP of the HTTP request. • Auto (JS Cookie): The Web browser will finish the authentication process automatically. • Auto (Redirect): The Web browser will finish the authentication process automatically. • Manual (Access Configuration): The initiator of the HTTP request must confirm by clicking OK on the returned page to finish the authentication process.

Option	Description
	• Manual (CAPTCHA): The initiator of the HTTP request must be confirmed by entering the authentication code on the returned page to finish the authentication process. • Crawler-friendly: When the authentication method is selected as **Auto (JS Cookie)**, **Auto (Redirect)**, **Manual (Access Configuration)** or **Manual (CAPTCHA)**, you can enable the Crawler-friendly function. If this button is clicked, system will not authenticate to the crawler. • Request limit: Specifies the request limit for the HTTP request flood protection. After configuring the request limit, system will limit the request rate of each source IP. If the request rate is higher than the limitation specified here and the HTTP request flood protection is enabled, system will handle the exceeded requests according to the action specified (Block IP/Reset). To record a log, click the Record log enable button. • Proxy limit: Specifies the proxy limit for the HTTP request flood protection. After configuring the proxy limit, system will check whether each source belongs to the each source IP proxy server. If belongs to, according to configuration to limit the request rate. If the request rate is higher than the limitation specified here and the HTTP request flood protection is enabled, system will

Option	Description
	handle the exceeded requests according to the action specified (Block IP/Reset). To record a log, click the Record log enbale button. • White List: Specifies the white list for the HTTP request flood protection. The source IP added to the white list will not check the HTTP request flood protection. **Note**: Non-root VSYS does not support the HTTP Request Flood Protection.

8. In the Password Protection section, click ▸ next to **Password Protection** to expand this section, including Weak Password Detection, Brute Force, HTTP Plain Text Detection, and HTTP Password Protect Configuration.



   i. Turn on the **Weak Password Detection** switch to enable this function. Then, the system checks the strength of the plaintext password which is set under the FTP/Telnet/POP3/IMAP/SMTP/HTTP protocols in this profile. The password is detected as weak if it meets the conditions configured in the Weak Password Detection section. In this case, the system issues an alarm log to prevent potential security risks caused by a weak password. Click Configure to configure the detection parameters of the weak password.

   Note: When SSL proxy is configured in the policy, you can detect weak password

for encrypted protocols such as HTTP.

Configure the detection parameters of the weak password.

Option	Description
Password Length	Specify the length criterion of the password. If a password is shorter than the length criterion, it will be detected as a weak password. The default length criterion is 6 characters. You can specify the password length criterion from 6 characters to 50 characters.
Password Character Type	Specify how many character types should be covered in the password. There are four types of characters: digits, uppercase letters, lowercase letters, and symbols. If the character types covered in a password are less than the specified number, the password will be detected as a weak password. By default, the system will detect the password containing less than 2 character types as a weak password and you can specify up to 4 character types for the detection of the password character type.
Other situations:	In the following situations, the password will be detected as a weak password: User Name Equals Password, Continuous Character Detection, FTP Anonymous Login Detection. • **User Name Equals Password**: The password that equals the user name will be detected as a weak password after the detection function is enabled. • **Continuous Character Detection**: After this detection is enabled, a password that has less than 10 characters, among which at least 8 characters are the

Option	Description
	same or in consecutive sequence, will be detected as a weak password, such as 1aaaaaaaa, 1abcdefgh, a87654321. • **FTP Anonymous Login Detection**: When you log in anonymously through FTP, the system identifies your password as a weak password.
Specify Weak Password	You can specify the weak passwords. If a password matches the specified weak password, the system will consider the password as a weak one. You can specify up to 100 weak passwords.

ii. Click **Configure** next to **Brute Force** to go to the **Brute Force** panel. You can configure to block the brute force attacks under the FTP/MSRPC/POP3/SMTP/SUNRPC/Telnet/IMAP/SSH/LDAP/SMB/VNC/RDP/HTTP protocol.
Note: The blacklist of brute-force attack IP does not take effect after the system is restarted.

To configure the protocol, click the Enable button behind the protocol. To enable/disable all protocols, click Enable All or Disable All.

Option	Description
FTP/MSRPC/ POP3/SMTP/ SUNRPC/Telnet/ IMAP/SSH/	**Action for Brute-force**: If the login attempts per 5 minutes fail for the times specified by the threshold, system will identify the attempts as an intrusion and take an action according to the con-

Option	Description
LDAP/SMB/ VNC/RDP	figuration. Click the **Enable** button to enable brute-force. • Login Threshold per 5 Mins: Specifies a permitted authentication/login failure count per 5 minutes. • Action: Block the IP address of the attacker • Block Time: Specifies the block duration. Default value: 60. Valid values: 60 to 3600. Unit: Second. • Time Unit: If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address or the service of the attacker.

iii. Turn on the **HTTP Plain Text Detection** switch to enable this function. Then, the system checks the password field in the HTTP packet. If the password is not encrypted, an alarm log is generated.
Note: When the login is successful, the system performs plaintext detection only against the password in the HTTP packet but not the HTTPs packet because the HTTPS protocol is not transmitted in plaintext by default.

iv. In the **HTTP Password Protect Configuration** section, you can configure the username field , password field, success-login response code, success-login field, fail-login response code, and fail-login field in the HTTP login packet. The system can

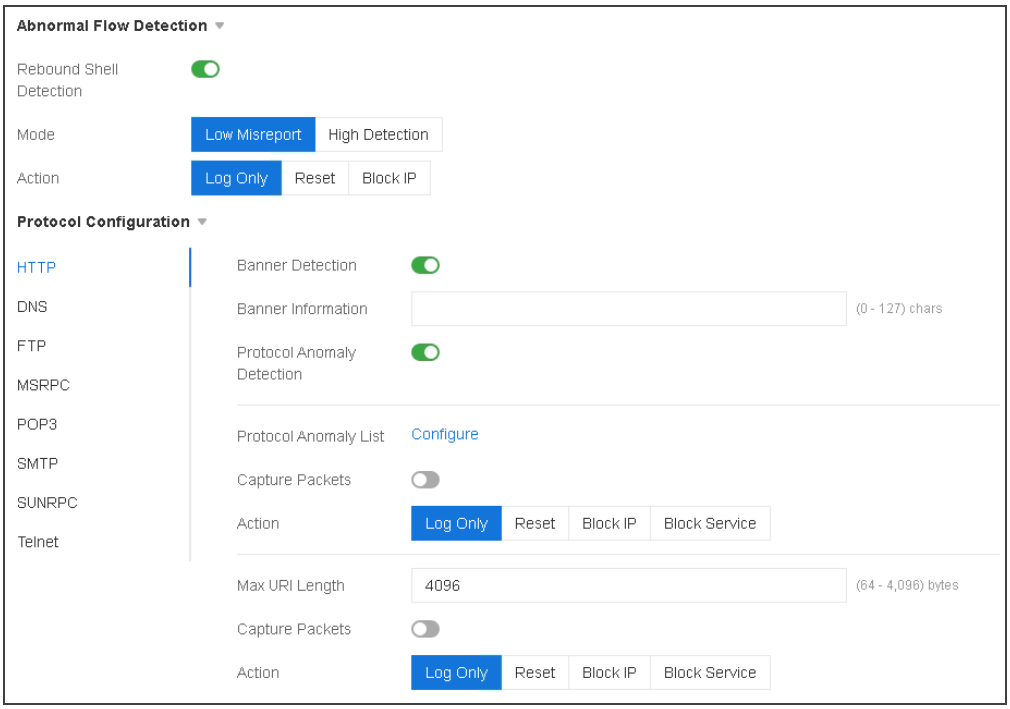
determine whether the login password is weak and whether there is brute-force attack by parsing the username, password, and login results contained in the HTTP login packet. The system is configured with a list of default username field, password field, and login result fields. However, the content of the HTTP protocol depends on the negotiation between the client and the server, therefore, to avoid false negatives, you can customize fields that tell information about the username, password, successful login, and failed login in the actual HTTP packet. This way, the system detects weak password and brute-force attacks and perform corresponding actions according to the configured rules.

Configure the following options in the HTTP Password Protect Configuration.

Option	Description
Username Field(s)	Specifies the username field in the HTTP login packet. The username field is case insensitive. Multiple fields can be separated with a semicolon. For example, username;user;usrname;j_username.
Password Field(s)	Specifies the password field in the HTTP login packet. The password field is case insensitive. Multiple fields can be separated with a semicolon. For example, password;passwd;pass;pwd;j_password.
Success-login Response Code(s)	Specifies the success-login response code(s) in the HTTP login packet. Multiple codes can be separated with a semicolon. For example, 200;302;201.
Success-	Specifies the success-login field in the HTTP login

Option	Description
login Field(s)	packet. The success-login field is case insensitive. Multiple fields can be separated with a semicolon. For example, loginsuccess;login-success.
Fail-login Response Code(s)	Specifies the fail-login response code(s) in the HTTP login packet. Multiple codes can be separated with a semicolon. For example, 200;302;201;303.
Fail-login Field(s)	Specifies the fail-login field in the HTTP login packet. The fail-login field is case insensitive. Multiple fields can be separated with a semicolon. For example, login-error;login-error;loginerr.

9. In the **Abnormal Flow Detection** section, click ▸ next to **Abnormal Flow Detection** to expand this section, including **Rebound Shell Detection and Protocol Configuration**.



i. Turn on the switch next to Rebound Shell Detection and configure this function.

Option	Description
Action	Specifies the defend action against the rebound shell attacks. • Log Only - The system only generate logs when it detects the rebound shell attacks. • Reset - When a rebound shell attack is detected, the system resets connection (TCP) or sends destination unreachable packets (UDP), and then generates logs. • Block IP - Block the IP address of the rebound shell attacker and configure the block time. • Block Time: The default value is 60 seconds. The value range is from 60 to 3600 seconds. If longer block duration is needed, you can select bigger time unit, such as Hour or Day. You can also block the attacker IP permanently.
Mode	Specifies the detect and defend mode for the rebound shell attacks. • Low Misreport: When the system scans to detect keywords of the rebound shell attack, logs are reported only when the keywords are hit more than four

Option	Description
	time. This mode can be used in scenarios where high system performance is required. • High Detection: When the system scans to detect keywords of the rebound shell attack, logs are reported when the keywords are hit more than twice. This mode can be used in scenarios with high requirements for attack detection.

ii. Click ▸ next to **Protocol Configuration**. System supports the configurations of HTTP, DNS, FTP, MSRPC, POP3, SMTP, SUNRPC, and Telnet.

In the HTTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against FTP server banners. • Banner Information: Type the new information into the box that will replace the original server banner information
Protocol Anomaly Detection	Select **Enable** to analyze the HTTP packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the **Protocol Anomaly List** panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules.

Option	Description

	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	  • Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking

Option	Description
	duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max URI Length**: Specify a max URI length for the HTTP protocol. If the URI length exceeds the limitation, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

In the DNS tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Select **Enable** to analyze the DNS packets. If abnormal contents exist, you can:
	Protocol Anomaly list: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action:

Option	Description

	• Log Only - Record a log;
	• Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	• Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.

In the FTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against FTP server banners. • Banner Information: Type the new information into the box that will replace the original server banner information
Protocol Anomaly Detection	Select **Enable** to analyze the FTP packets. If abnormal contents exist, you can:

	Protocol Anomaly list: Click **Configure** to open the **Protocol Anomaly List** panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click Disable to disable the rules.
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;

Option	Description
	• Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker. • Block Service - Block the service of the attacker and specify a block duration. • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
	Max Command Line Length: Specifies a max length (including carriage return) for the FTP command line. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

Option	Description
	Max Response Line Length: Specifies a max length for the FTP response line.If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

In the MSRPC tab, configure the following settings:

Option	Description

Protocol Anomaly Detection	Select **Enable** to analyze the MSRPC packets. If abnormal contents exist, you can:
	Protocol Anomaly list: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules.
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;

Option	Description

	• Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
	Max Bind Length: Specifies a max length for MSRPC's binding packets. If the length exceeds the limits, you can:
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log.

Option	Description
	• Action: Log Only; Reset; Block IP; Block Service. **Max Request Length**: Specifies a max length for MSRPC's request packets. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

	Protocol Anomaly list: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules.
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid

Option	Description
	values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker. • Block Service - Block the service of the attacker and specify a block duration. • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
	Max Bind Length: Specifies a max length for MSRPC's binding packets. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.
	Max Request Length: Specifies a max length for MSRPC's request packets. If the length exceeds the limits, you can:

Option	Description
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

In the POP3 tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against POP3 server banners. • Banner information - Type the new information into the box that will replace the original server banner information.
Protocol Anomaly Detection	Click the **Enable** button to analyze the POP3 packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click **Disable** to disable the rules. • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: • Log Only - Record a log;

Option	Description

	• Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	• Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.
	Max Command Line Length: Specifies a max length (including carriage return) for the POP3 command line. If

Option	Description
	the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service. **Max Parameter Length**: Specifies a max length for the POP3 client command parameter. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service. **Max Failure Times**: Specifies a max failure time (within one single POP3 session) for the POP3 server. If the failure time exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

In the SMTP tab, configure the following settings:

Option	Description
Banner Detection	Click the **Enable** button to enable protection against SMTP server banners. • Banner information - Type the new information into

Option	Description
	the box that will replace the original server banner information.

Protocol Anomaly Detection	Click **Enable** to analyze the SMTP packets. If abnormal contents exist, you can:
	Protocol Anomaly list: Click Configure to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click Enable to enable the rules; and click Disable to disable the rules.
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater dur-

Option	Description
	ation unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker. • Block Service - Block the service of the attacker and specify a block duration. • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Max Command Line Length**: Specifies a max length (including carriage return) for the SMTP command line. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service. **Max Path Length**: Specifies a max length for the reverse-path and forward-path field in the SMTP client command. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log.

Option	Description
	• Action: Log Only; Reset; Block IP; Block Service. **Max Reply Line Length**: Specifies a max length reply length for the SMTP server. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service. **Max Text Line Length**: Specifies a max length for the E-mail text of the SMTP client. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service. **Max Content Type Length**: Specifies a max length for the content-type of the SMTP protocol. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service. **Max Content Filename Length**: Specifies a max length for the filename of E-mail attachment. If the length exceeds the limits, you can:

Option	Description
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service. **Max Failure Time**: Specifies a max failure time (within one single SMTP session) for the SMTP server. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

In the SUNRPC tab, configure the following settings:

Option	Description
Protocol Anomaly Detection	Click **Enable** to analyze the SUNRPC packets. If abnormal contents exist, you can: **Protocol Anomaly list**: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules. • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: • Log Only - Record a log;

Option	Description

	• Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	• Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the IP address of the attacker.
	• Block Service - Block the service of the attacker and specify a block duration.
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker.

In the Telnet tab, configure the following settings:

Option	Description

Protocol Anomaly Detection	Click **Enable** to analyze the Telnet packets. If abnormal contents exist, you can:
	Protocol Anomaly list: Click **Configure** to open the Protocol Anomaly List panel, which will display the signature rules related to the HTTP protocol anomaly in this profile. Select one or more rules and click **Enable** to enable the rules; and click **Disable** to disable the rules.
	• Capture Packets: Capture the abnormal packets. You can view and download them in the threat log.
	• Action:
	  • Log Only - Record a log;
	  • Reset - Reset connections (TCP) or sends destination unreachable packets (UDP) and also generate logs;
	  • Block IP - Block the IP address of the attacker and specify a block duration;
	  • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently

Option	Description
	block the IP address of the attacker. • Block Service - Block the service of the attacker and specify a block duration. • Block Time: Default value: 60. Valid values: 60 to 3600. Unit: Second. If you want to specify a longer blocking duration, you can select a greater duration unit ("hour" or "day") , or you can select "permanent" to permanently block the service of the attacker. **Username/Password Max Length**: Specifies a max length for the username and password used in Telnet. If the length exceeds the limits, you can: • Capture Packets: Capture the abnormal packets. You can view and download them in the threat log. • Action: Log Only; Reset; Block IP; Block Service.

10. Click **Save** to complete the protocol configurations.

11. Click **OK** to complete the IPS rule configurations.

Notes: The IPS Capture Packets function is supported for A-series devices (except A1605/A1805/A2205) that are installed with SSD, .

Cloning an IPS Rule

System supports the rapid cloning of an IPS rule. The user can generate a new IPS rule by modifying some parameters of the cloned IPS rule.

To clone an IPS rule, take the following steps:

1. Select **Object > Intrusion Prevention System > Profile**.
2. Select an IPS rule in the list.
3. Click **Clone** above the list, the **Name** configuration box will appear below the button, enter the name of the cloned IPS rule.
4. A cloned IPS rule will be generated in the list.

IPS Global Configuration

Configuring the IPS global settings includes:

- Enable the IPS function
- Specify how to merge logs
- Specify the work mode

Click **Object > Intrusion Prevention System > Configuration** to configure the IPS global settings.

Option	Description
IPS	Click/clear the **Enable** button to enable/disable the IPS function.
Log Aggregate Type	System can merge log information that meets the aggregation rule. Thus it can help reduce the number of logs and avoid receiving redundant logs. You can configure the merging type of logs generated by the IPS function. The system supports the following four merging types:

Option	Description
	• Do Not Merge - Do not merge any logs. • Source IP - Merge the logs with the same Source IP. • Destination IP - Merge the logs with the same Destination IP. • Source IP, Destination IP - Merge the logs with the same Source IP and the same Destination IP. This is the default option.
Aggregate Time	Specifies the time granularity for IPS threat log of the same merging type (specified above) to be stored in the database. At the same time granularity, the same type of log is only stored once. It ranges from 10 to 600 seconds.
Mode	Specifies a working mode for IPS: • IPS - If attacks have been detected, StoneOS will generate logs, and will also reset connections or block attackers. This is the default mode. • Log only - If attacks have been detected, StoneOS will only generate logs, but will not reset connections or block attackers.
Record HTTP Proxy IP	Click **Enable** check box to enable the device to record HTTP proxy IP. After enabled, in the deployment scenario of HTTP proxy, when the device generates threat information (including threat logs and threat events), the attacker field in the threat information records the IP address of the HTTP proxy. After disabled, for threat information that has passed through the HTTP proxy, the attacker field in the threat information is recorded as the real IP address before the proxy. The function is enabled by default.

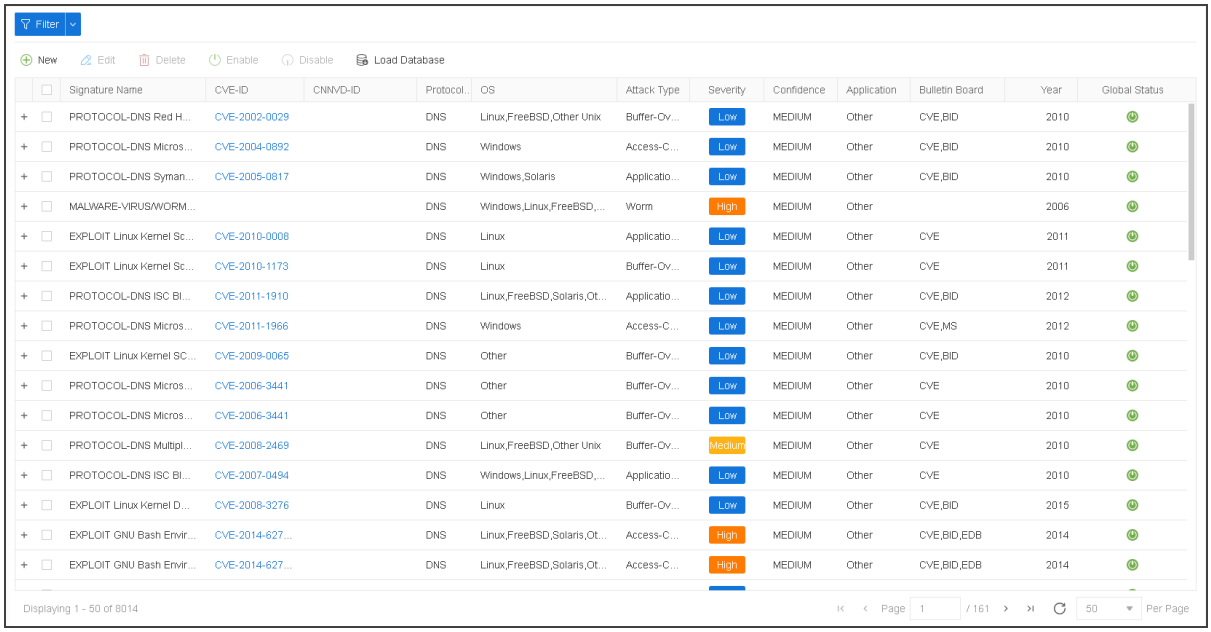
Option	Description
	Note: • This function only takes effect in the HTTP proxy deployment scenario and only for HTTP traffic. • This function only takes effect in the threat information generated by IPS filtering, otherwise will not takes effect.

After the configurations, click **OK** to save the settings.

Notes: Non-root VSYS does not support IPS global configuration.

Signature List

Select **Object > Intrusion Prevention System > Signature List**. You can see the signature list.



The upper section is for searching signatures. The lower section is for managing signatures.

Searching Signatures

In the upper section, click **Filter** to set the search conditions to search the signatures that match the condition.

To clear all search conditions, click **Remove All**. To save the search conditions, click  and then click **Save Filters** to name this set of search conditions and save it.

Managing Signatures

You can view signatures, create a new signature, load the database, delete a signature, edit a signature, enable a signature, and disable a signature.

- View signatures: In the signature list, click the "+" button before the ID of a signature to view the details.
- Create a new signature: click **New**.

  On the User-defined Signature page, configure the following settings:

Option	Description
Name	Specifies the signature name.
Description	Specifies the signature descriptions.
Protocol	Specifies the affected protocol.
Matching Direction	Specifies the matching direction of the signature. • To_Server means the package of attack is from the server to the client. • To_Client means the package of attack is from the client to the server. • Any includes To_Server and To_Client.

Option	Description
Attack Direction	Specifies how the system determines the direction of the attack traffic. Typically, this option works with Matching Direction. By default, the system determines the source IP address of the attack traffic as the attacker. For example, in the case where **Matching Direction** is set to **To Server**, and **Attack Direction** is set to **Source To Destination**, the system determines that the attack source comes from the client when an attack occurs. However, if **Matching Direction** is set to **To Server**, and **Attack Direction** is set to **Destination To Source**, the system determines that the attack source comes from the server.
Source Port	Specifies the source port of the signature. • Any - Any source port. • Included - The source port you specified should be included. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate. • Excluded - The source port you specified should be excluded. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate.
Destination Port	Specifies the destination port of the signature. • Any - Any destination port. • Included - The destination port you specified should be

Option	Description
	included. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate. • Excluded - The destination port you specified should be excluded. It can be one port, several ports, or a range. Specifies the port number in the text box, and use "," to separate.
Dsize	Specifies the payload message size. Select "----",">", "<" or "=" from the drop-down list and specifies the value in the text box. "----" means no setting of the parameters.
Severity	Specifies the severity of the attack.
Attack Type	Select the attack type from the drop-down list.
Application	Select the affected applications.
Operating System	Select the affected operating system from the drop-down list.
Bulletin Board	Select a bulletin board of the attack.
Year	Specifies the released year of attack.
Action	Specifies the default action for the signature - Log Only or Reset. If **Log Only** is selected, the system only generate logs when it detects an attack. If **Reset** is selected, the system resets connections (TCP) or sends destination unreachable packets (UDP), and generates logs when it detects an attack.
Detection Fil-	Specifies the frequency of the signature rule.

Option	Description
ter	• Track - Select the track type from the drop-down list. It can be **by_source** or **by_destination**. System will use the statistic of the source IP or the destination IP to check whether the attack matches this rule. • Count - Specifies the maximum times the rule occurs in the specified time. If the attacks exceed the Count value, system will trigger rules and act as specified. • Seconds - Specifies the interval value of the rule occurs.

Configure Content, click New to specify the content of the signature:

Option	Description
Content	Specifies the signature content. Select the following check box if needed: • HEX - Means the content is hexadecimal. • Case Insensitive - Means the content is not case sensitive. • URI - Means the content needs to match URI field of HTTP request.
Relative	Specifies the signature content location. • If **Beginning** is selected, system will search from the header of the application layer packet. • Offset: System will start searching after the offset from the header of the application layer packet. The unit is byte.

Option	Description
	• Depth: Specifies the scanning length after the offset. The unit is byte. • If **Last Content** is selected, system will search from the content end position. • Distance: System will start searching after the distance from the former content end position. The unit is byte. • Within: Specifies the scanning length after the distance. The unit is byte.

- Load the database: After you create a new signature, click **Load Database** to make the newly created signature take effect.
- Edit a signature: Select a signature and then click **Edit**. You can only edit the user-defined signature. After editing the signature, click **Load Database** to make the modifications take effect.
- Delete a signature: Select a signature and then click **Delete**. You can only delete the user-defined signature. After deleting the signature, click **Load Database** to make the deletion take effect.
- Enable/Disable signatures: After selecting signatures, click **Enable** or **Disable**.



Notes: Non-root VSYS does not support signature list.

Configuring IPS White list

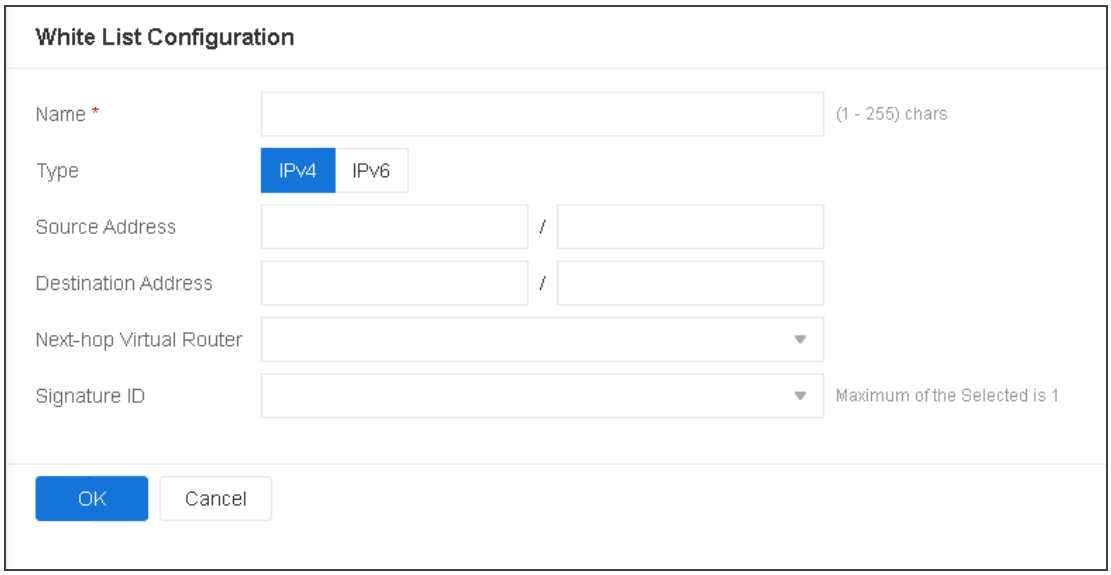
The device detects the traffic in the network in real time. When a threat is detected, the device generates alarms or blocks threats. With the complexity of the network environment, the threat of

the device will generate more and more warning, too much threat to the user can not start making the alarm, and many of them are false positives. By providing IPS whitelist, the system no longer reports alarms or blocks to the whitelist, thus reducing the false alarm rate of threats. The IPS whitelist consists of source address, destination address, and threat ID, and the user selects at least one item for configuration.

To configure an IPS white list :

1. Select **Object> Intrusion Prevention System >Whitelist**

2. Click **New**.



Option	Description
Name	Specifies the white-list name.
Type	Select the address type, including IPv4 or IPv6.
Source Address	Specifies the source address of the traffic to be matched by IPS.
Destination Address	Specifies the destination address of the traffic to be matched by IPS.
Next-hop Vir-	Select the Next-hop VRouter from the drop-down list.

Option	Description
tual Router	
Signature ID	Select the signature ID from the drop-down list. A whitelist can be configured with a maximum of one threat ID. When the threat ID is not set, the traffic can be filtered based on the source and destination IP address. When user have configured threat ID, the source address, destination address and threat ID must be all matched successfully before the packets can be released.

3. Click **OK**.

Sandbox

A sandbox executes a suspicious file in a virtual environment, collects the actions of this file, analyzes the collected data, and verifies the legality of the file.

The Sandbox function of the system uses the cloud sandbox and the local sandbox technology. The suspicious file will be uploaded to the cloud sandbox or the local sandbox. The cloud sandbox or the local sandbox will collect the actions of this file, analyze the collected data, verify the legality of the file, give the analysis result to the system and deal with the malicious file with the actions set by system.

The Sandbox function contains the following parts:

- Collect and upload the suspicious file: The Sandbox function parses the traffic, and extracts the suspicious file from the traffic.
    - If there are no analyze result about this file in the local database, system will upload this file to the local sandbox or to the Hillstone cloud service platform, and the local sandbox will analyze the file or the cloud service platform will upload the suspicious file to

the cloud sandbox for analysis. For how to connect to the Hillstone cloud service platform, refer to "Connecting to Hillstone Cloud Service Platform" on Page 1770.

- If this file has been identified as an illegal file in the local database of the Sandbox function, system will generate corresponding threat logs and cloud sandbox logs.

Additionally, you can specify the criteria of the suspicious files by configuring a sandbox profile.

- Check the analysis result and take actions: The Sandbox function checks the analysis results of the suspicious file returned from the cloud sandbox or the local sandbox, verifies the legality of the file, saves the result to the local database. If this suspicious file is identified as an illegal file, you need to deal with the file according to the actions (reset the connection or report logs) set by system. If it's the first time to find malicious file by the cloud sandbox or the local sandbox, system will record threat logs and cloud sandbox logs and cannot stop the malicious link. When malicious file accesses the cached threat information in the local device, the threat will be effective only by resetting connection.
- Maintain the local database of the Sandbox function: Record the information of the uploaded files, including uploaded time and analysis result. This part is completed by the Sandbox function automatically.

Notes: The cloud sandbox function is controlled by license. To use the cloud sandbox function, install the cloud sandbox license.

Related Topics: Configuring Sandbox

Configuring Sandbox

This chapter includes the following sections:

- Preparation for configuring the Sandbox function
- Configuring the Sandbox rules
- Sandbox global configurations

Preparation

Before enabling the Sandbox function, make the following preparations:

Make sure your system version supports the Sandbox function.

The current device is registered to the Hillstone cloud service platform. For how to connect to the Hillstone cloud service platform, refer to "Connecting to Hillstone Cloud Service Platform" on Page 1770.

Import the cloud sandbox license and reboot. The cloud sandbox function will be enabled after rebooting.



Notes: After the Sandbox function is enabled, system's max concurrent sessions might decrease. For more information about the maximum concurrent sessions, see "The Maximum Concurrent Sessions" on Page 1847.

Configuring Sandbox

The System supports the zone-based and policy-based Sandbox:

- If a security zone is configured with the Sandbox function, system will perform sandbox detection on the traffic that is sourced from or destined to the binding zone specified in the rule.
- If a policy rule is configured with the Sandbox filtering function, system will perform sandbox detection on the traffic that is destined to the policy rule you specified.

- The sandbox configurations in a policy rule are superior to that in a zone rule if they are specified at the same time, and the sandbox configurations in a destination zone are superior to that in a source zone if they are specified at the same time.

The system also supports binding the sandbox profile to a ZTNA policy to perform sandbox detection and processing on the traffic matching the ZTNA policy. For configuration information, refer to Configuring ZTNA Policy.

To create the zone-based Sandbox, take the following steps:

1. Create a zone. For more information , refer to Security Zone.
2. In the Zone Configuration page, expand Threat Protection.
3. Click the **Enable** button after the **Sandbox**. Select a existing Sandbox rule from the profile drop-down list or click the "+" button to create a sandbox rule you need.
4. Click **OK**.

To create the policy-based Sandbox, take the following steps:

1. Click **Object > Sandbox > Configuration**. Click the **Enable** button after the Cloud Sandbox or the Local Sandbox to enable the Sandbox function. If you do not have a cloud sandbox license, you can enable the Free Cloud Sandbox function. The Free Cloud Sandbox function only supports to detect PE files.
2. Click **Object > Sandbox > Profile** to create a sandbox rule you need.
3. Bind the sandbox rule to a policy. Click **Policy > Security Policy**.Select the policy rule you want to bind or click **New** to create a new policy. In the Policy Configuration page, expand **Protection** and then click the **Enable** button of Sandbox. Select a existing Sandbox rule from the drop-down list or click the "+" button to create a sandbox rule you need.

Configuring a Sandbox Rule

A sandbox rule contains the files types that device has detected, the protocols types that the device has detected, the white list settings, and the file filter settings.

- File Type: Support to detect PE, APK, JAR, MS-Office, PDF, SWF, RAR, ELF, ZIP, Script, and Others file. "Others" indicates all other types, except the ones that you can select on the page.
- Protocol Type: Support to detect HTTP, FTP, POP3, SMTP, IMAP4 and SMB protocol. If SMB protocol type is used, the system supports the filtering and blocking of files in break-point resumption scenarios.
- White list: A white list includes domain names that are safe. When a file extracted from the traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox or the local sandbox.
- File filter: Mark the file as a suspicious file if it satisfies the criteria configured in the file filter settings. The analysis result from the cloud sandbox tor he local sandbox determines whether this suspicious file is legal or not.
- Actions: When the suspicious file accesses the threat items in the sandbox, system will deal with the malicious file with the set actions.

There are five built-in sandbox rules with the files and protocols type configured, white list enabled and file filter configured. The four default sandbox rules includes predef_low, predef_ middle, predef_high, predef_pe and no_sandbox.

- **predef_low**: A loose sandbox detection rule, whose file type is PE and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, with white list and file filter enabled.
- **predef_middle**: A middle-level sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, with white list and file filter enabled.

- **predef_high**: A strict sandbox detection rule, whose file types are PE/APK/JAR/MS-Office/PDF/SWF/RAR/ZIP/ELF/Script and protocol types are HTTP/FTP/POP3/SMTP/IMAP4/SMB, , with white list and file filter enabled.
- **predef_pe**: A sandbox detection rule, whose file type is only PE and protocol types are HTTP/FTP/POP3/SMTP/IMAP4, with white list and file filter enabled.
- **no_sandbox**:With this detection rule, the system does not perform any sandbox detection.

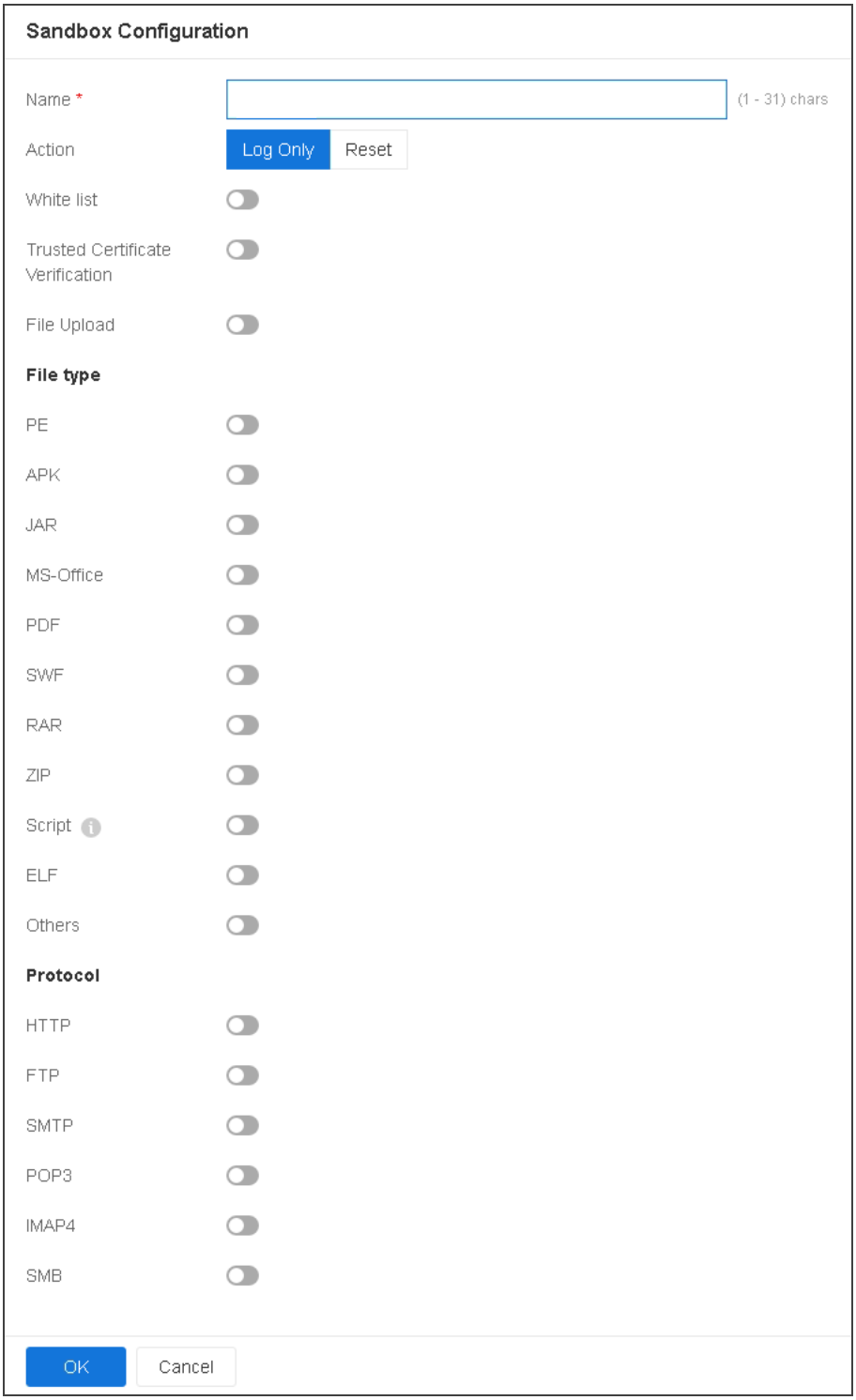


Notes: When the SSL proxy function is enabled, the system will support sandbox detection of HTTPS/POP3S/SMTPS/IMAPS traffic.

To create a new sandbox rule, take the following steps:

1. Select **Object > Sandbox > Profile**.

2. Click **New** to create a new sandbox rule. To edit an existing one, select the check box of this rule and then click **Edit**.


Sandbox Configuration
Name *
(1 - 31) chars
Action
Log Only
Reset
White list
Trusted Certificate Verification
File Upload
File type
PE
APK
JAR
MS-Office
PDF
SWF
RAR
ZIP
Script
ELF
Others
Protocol
HTTP
FTP
SMTP
POP3
IMAP4
SMB
OK
Cancel

Option	Description
Name	Enter the name of the sandbox rule.
Action	When the suspicious file accesses the threat items in the local sandbox, system will deal with the malicious file with the set actions. Actions: • Log Only - When detecting malicious files, system will pass traffic and record logs only (threat log and cloud sandbox log). • Reset - When detecting malicious files, system will reset connection of malicious link and record threat logs and cloud sandbox logs only.
White List	Click **Enable** to enable the white list function. A white list includes domain names that are safe. When a file extracted from the traffic is from a domain name in the white list, this file will not be marked as a suspicious file and it will not be upload to the cloud sandbox. You can update the white list in **System > Upgrade Management > Signature Database Update > Sandbox Whitelist Database Update**.
Trusted Certificate Verification	Click **Enable** to enable the verification for the trusted certification. After enabling, system will not detect the PE file whose certification is trusted.
File Upload	By default, the file will be uploaded to the cloud sandbox when it marks it is classified as suspicious. You can disable the function of suspicious file uploading, which will prevent the sus-

Option	Description
	picious file from being uploaded to the cloud sandbox. Click the **Disable** to disable the function of suspicious file uploading.
File Filter: Mark the file as a suspicious file if it satisfies the criteria configured in the file filter settings. The analysis result from the cloud sandbox determines whether this suspicious file is legal or not. The logical relation is AND.	
File Type	Mark the file of the specified file type as a suspicious file. Click the **Enable** button of the file type, select **Cloud Sandbox Detection** to specify that suspicious files will be uploaded to the cloud sandbox for detection, or select **Local Sandbox Detection** to specify that suspicious files will be uploaded to the local sandbox for detection. The system can mark the PE(.exe), APK, JAR, MS-Office, PDF, SWF, ELF, RAR, ZIP, Script and Others (all types other than the preceding types) file as a suspicious file now. Files of the Others type can only be uploaded to the local sandbox but not the cloud sandbox for detection. If no file type is specified, the Sandbox function will mark no file as a suspicious one.
Protocol	Specifies the protocol to scan. System can scan the HTTP, FTP, POP3, SMTP, IMAP4 and SMB traffic now. If no protocol is specified, the Sandbox function will not scan the network traffic. After specifying the protocol type, you have to specify the direction of the detection: • **Upload** - The direction is from client to server. • **Download** - The direction is from server to client.

Option	Description
	• **Bi-directional** - The direction includes uploading and downloading directions.

3. Click **OK** to save the settings.

Threat List

The threat list means the list of threat items in the Hillstone device. There are three sources of the threat items:

- The Hillstone device finds suspicious file and upload this file to the local sandbox or to the cloud sandbox. After verifying the file is malicious, the cloud sandbox or the local sandbox will send the analysis results and MD5 to the device, and the threat item will be listed in the threat list.
- The Hillstone device finds suspicious file and successfully queries MD5 of the threat in the cloud sandbox or the local sandbox, the threat item will be listed in the threat list.
- The Hillstone device receives the synchronous threat MD5 from the Hillstone cloud service platform and matches the threat, the threat item will be listed in the threat list.

You can filter and check threat items through specifying MD5 or the name of virus on the threat list page, as well as add the selected threat item to trust list. Take the following steps:

1. Click **Object > Sandbox > Threat List**.
2. Select the threat item that needs to be added to the trust list and click **Add to Trust** button. When threat item is added, once it's matched, the corresponding traffic will be released.

Trust List

You can view all the sandbox threat information which can be detected on the device and add them to the trust list. Once the item in trust list is matched, the corresponding traffic will be released and not controlled by the actions of sandbox rule.

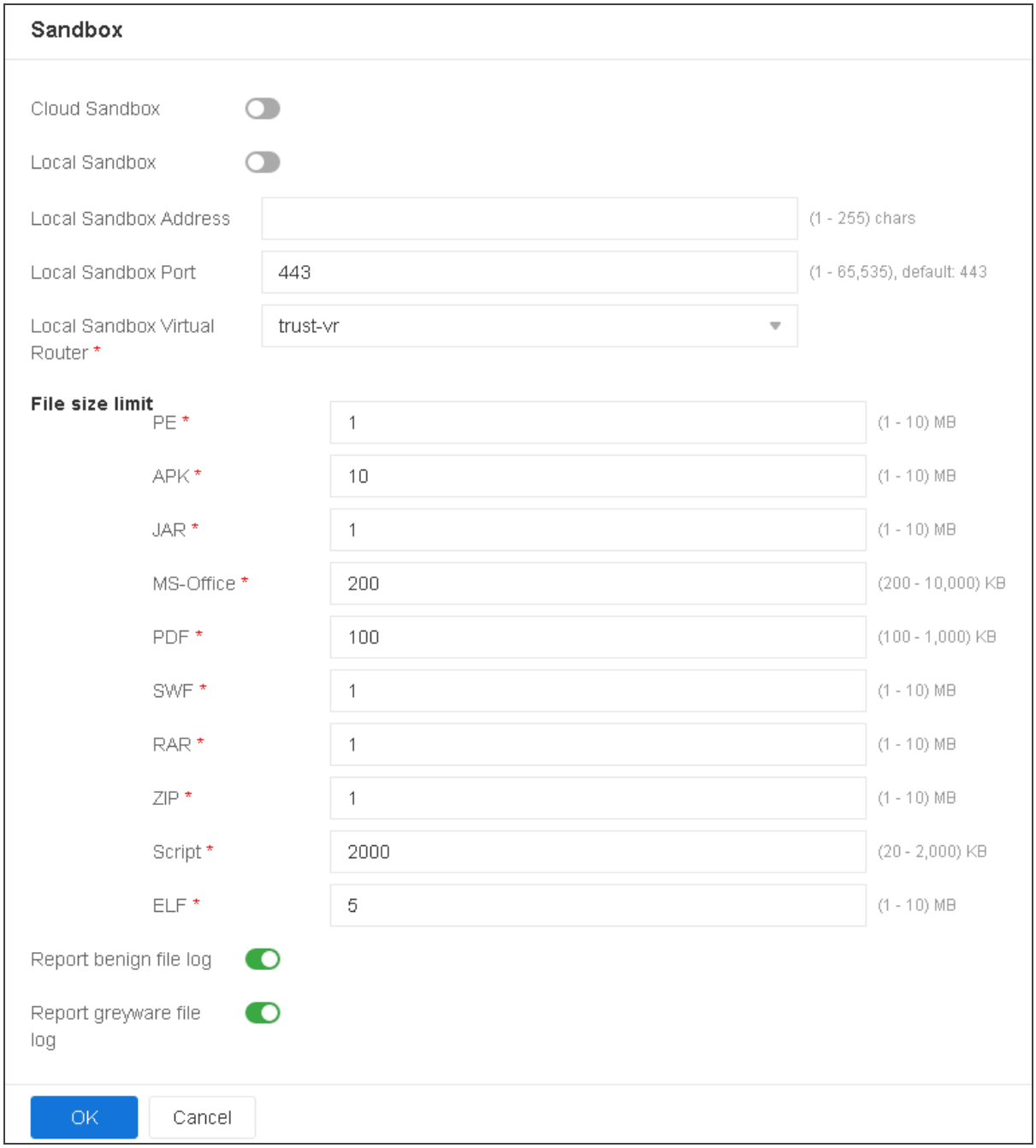
To remove threat items in the trust list, take the following steps:

1. Click **Object > Sandbox > Trust List**.
2. Select the threat item that needs to be removed in the trust list and click **Remove from Trust** button. The threat item will be removed from the trust list.

Sandbox Global Configurations

To configure the sandbox global configurations, take the following steps:

1. Select **Object > Sandbox > Configuration**.



2. Click the **Enable** button of Cloud Sandbox to enable the cloud sandbox function. If you do not have a cloud sandbox license, you can enable the Free Cloud Sandbox function. The Free Cloud Sandbox function only supports to detect PE files.

3. Click the **Enable** button of Local Sandbox to enable the local sandbox function., and then specifies the IP address and the VRouter for the local sandbox.Specify the file size for the files you need. The file that is smaller than the specified file size will be marked as a suspicious file.
4. Specify the file size for the files you need. The file that is smaller than the specified file size will be marked as a suspicious file.
5. If you click the **Report benign file log** button, system will record cloud sandbox logs of the file when it marks it as a benign file. By default, system will not record logs for the benign files.
6. If you click the **Report greyware file log** button, system will record cloud sandbox logs of the file when it marks it as a greyware file. A greyware file is the one system cannot judge it is a benign file or a malicious file. By default, system will not record logs for the greyware files.
7. Click **OK** to save the settings.

Attack-Defense

There are various inevitable attacks in networks, such as compromise or sabotage of servers, sensitive data theft, service intervention, or even direct network device sabotage that causes service anomaly or interruption. Security gates, belonging to a category of network security devices, must be designed with attack defense functions to detect various types of network attacks, and take appropriate actions to protect the Intranet against malicious attacks, thus assuring the normal operation of the Intranet and systems.

Devices provide attack defense functions based on security zones, and can take appropriate actions against network attacks to assure the security of your network systems.

ICMP Flood and UDP Flood

An ICMP Flood/UDP Flood attack sends huge amounts of ICMP messages (such as ping)/UDP packets to a target within a short period and requests for a response. Due to the heavy load, the

attacked target cannot complete its normal transmission task.

ARP Spoofing

LAN transmits network traffic based on MAC addresses. ARP spoofing attacks occur by filling in the wrong MAC address and IP address to make a wrong corresponding relationship of the target host's ARP cache table. This will lead to the wrong destination host IP packets, and the packet network's target resources will be stolen.

SYN Flood

Due to resource limitations, a server will only permit a certain number of TCP connections. SYN Flood just makes use of this weakness. During the attack an attacker will craft a SYN packet, set its source address to a forged or non-existing address, and initiate a connection to a server. Typically the server should reply the SYN packet with SYN-ACK, while for such a carefully crafted SYN packet, the client will not send any ACK for the SYN-ACK packet, leading to a half-open connection. The attacker can send large amount of such packets to the attacked host and establish are equally large number of half-open connections until timeout. As a result, resources will be exhausted and normal accesses will be blocked. In the environment of unlimited connections, SYN Flood will exhaust all the available memory and other resources of the system.

WinNuke Attack

A WinNuke attack sends OOB (out-of-band) packets to the NetBIOS port (139) of a Windows system, leading to NetBIOS fragment overlap and host crash. Another attacking vector is ICMP fragment. Generally an ICMP packet will not be fragmented; so many systems cannot properly process ICMP fragments. If your system receives any ICMP fragment, it's almost certain that the system is under attack.

IP Address Spoofing

IP address spoofing is a technology used to gain unauthorized access to computers. An attacker sends packets with a forged IP address to a computer, and the packets are disguised as if they were from a real host. For applications that implement validation based on IP addresses, such an

attack allows unauthorized users to gain access to the attacked system. The attacked system might be compromised even if the response packets cannot reach the attacker.

ICMP Redirect Attack

An ICMP redirect message is an out-of-band message that is designed to inform a host of a more optimal route through a network, but possibly used maliciously for attacks that redirect traffic to a specific system. In this type of an attack, the hacker, posing as a router, sends an ICMP redirect message to a host, which indicates that all future traffic must be directed to a specific system as the more optimal route for the destination.

IP Address Sweep and Port Scan

This kind of attack makes a reconnaissance of the destination address and port via scanners, and determines the existence from the response. By IP address sweeping or port scanning, an attacker can determine which systems are alive and connected to the target network, and which ports are used by the hosts to provide services.

Ping of Death Attack

Ping of Death is designed to attack systems by some over-sized ICMP packets. The field length of an IP packet is 16 bits, which means the max length of an IP packet is 65535 bytes. For an ICMP response packet, if the data length is larger than 65507 bytes, the total length of ICMP data, IP header (20 bytes) and ICMP header (8 bytes) will be larger than 65535 bytes. Some routers or systems cannot properly process such a packet, and might result in crash, system down or reboot.

Teardrop Attack

Teardrop attack is a denial of service attack. It is a attack method based on morbid fragmented UDP packets, which works by sending multiple fragmented IP packets to the attacker (IP fragmented packets include the fragmented packets of which packet, the packet location, and other information). Some operating systems contain overlapping offset that will crash, reboot, and so on when receiving fragmented packets.

Smurf Attack

Smurf attacks consist of two types: basic attack and advanced attack. A basic Smurf attack is used to attack a network by setting the destination address of ICMP ECHO packets to the broadcast address of the attacked network. In such a condition all the hosts within the network will send their own response to the ICMP request, leading to network congestion. An advanced Smurf attack is mainly used to attack a target host by setting the source address of ICMP ECHO packets to the address of the attacked host, eventually leading to host crash. Theoretically, the more hosts in a network, the better the attacking effect will be.

Fraggle Attack

A fraggle attack is basically the same with a smurf attack. The only difference is the attacking vector of fraggle is UDP packets.

Land Attack

During a Land attack, an attacker will carefully craft a packet and set its source and destination address to the address of the server that will be attacked. In such a condition the attacked server will send a message to its own address, and this address will also return a response and establish a Null connection. Each of such connections will be maintained until timeout. Many servers will crash under Land attacks.

IP Fragment Attack

An attacker sends the victim an IP datagram with an offset smaller than 5 but greater than 0, which causes the victim to malfunction or crash.

IP Option Attack

An attacker sends IP datagrams in which the IP options are abnormal. This attack intends to probe the network topology. The target system will break down if it is incapable of processing error packets.

Huge ICMP Packet Attack

An attacker sends large ICMP packets to crash the victim. Large ICMP packets can cause memory allocation error and crash the protocol stack.

TCP Flag Attack

An attacker sends packets with defective TCP flags to probe the operating system of the target host. Different operating systems process unconventional TCP flags differently. The target system will break down if it processes this type of packets incorrectly.

DNS Query Flood Attack

The DNS server processes and replies to all DNS queries that it receives. A DNS flood attacker sends a large number of forged DNS queries. This attack consumes the bandwidth and resources of the DNS server, which prevents the server from processing and replying legal DNS queries.

DNS Reply Flood Attack

When the DNS server receives the reply message, it will process the message regardless whether it is valid. DNS reply flood is that the attacker sends a large number of DNS reply message to the DNS cache server, causing the cache server to run out of resources by processing these reply messages.

TCP Split Handshake Attack

When a client establishes TCP connection with a malicious TCP server, the TCP server will respond to a fake SYN packet and use this fake one to initialize the TCP connection with the client. After establishing the TCP connection, the malicious TCP server switches its role and becomes the client side of the TCP connection. Thus, the malicious traffic might enter into the intranet.

SIP Flood

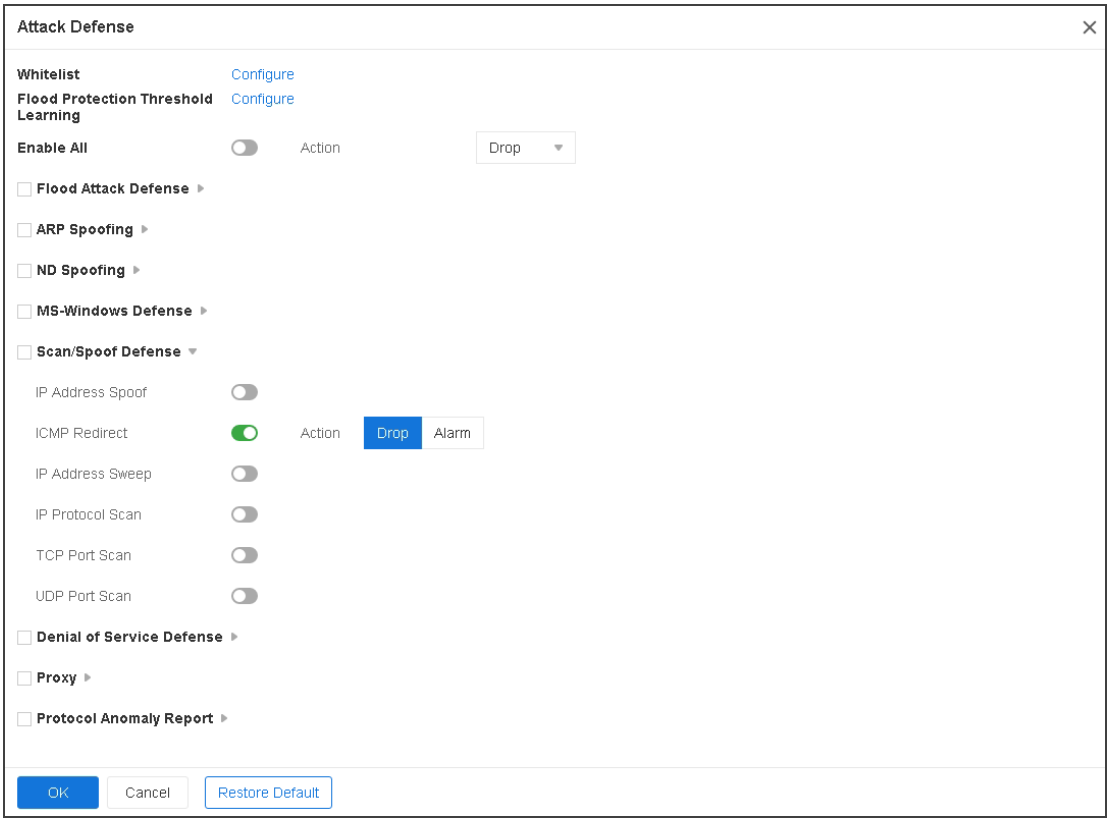
SIP (Session Initiation Protocol) is an application-layer signaling control protocol. It is used to initiate, modify and terminate interactive multimedia sessions, such as multimedia meetings and

Internet telephone. The attacker of the SIP flood attack sends a large number of INVITE messages to the target SIP server in a short time. Therefore, the target SIP server exhausts its resources and fails to respond to the call requests from valid users.

Configuring Attack Defense

To configure the Attack Defense based on security zones, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. On the Zone Configuration page, expand Threat Protection.
3. To enable the Attack Defense functions, click the **Enable** button, and click **Configure**.



Option	Description
Whitelist	IP address or IP range in the whitelist is exempt from attack defense check.

Option	Description
	Click **Configure**,and in the White Configuration tab, click **New** to create a whitelist. Select the type for the whitelist, including source whitelist and destination whitelist. And then select the IP type, including: • IP/Netmask - Specifies the IPv4 address and netmask. • IPv6/Prefix - Specifies the IPv6 address and prefix, range 120 to 128. • Address entry - Specifies the address entry.
Flood Protection Threshold Learning	An appropriate attack detection threshold is crucial for configuring attack defense. Flood protection threshold learning collects statistics on the maximum rate of traffic that passes through a normal network environment. Then, this function provides a proper reference value for the attack detection threshold. The Flood Protection Threshold Learning function is supported for SYN flood attacks, DNS Query flood attacks, DNS Recursive Query flood attacks, DNS Reply flood attacks, UDP flood attacks, ICMP flood attacks, and SIP flood attacks. For more information, see Configuring Flood Protection Threshold Learning.
Enable All	**Enable all**: Click this button to enable all the Attack Defense functions for the security zone. **Action**: Specifies an action for all the Attack Defense functions, i.e., the defense measure system will be taken if any attack has been detected. • Drop - Drops packets. This is the default action.

Option	Description
	• Alarm - Gives an alarm but still permits packets to pass through. • Do not specify global actions.
Flood Attack Defense	Click the ▶ button to expand the information of all flood attack defenses. Select the **Flood Attack Defense** check box to enable all flood attack defenses.
	ICMP Flood: Click this button to enable ICMP flood defense for the security zone. • Threshold - Specifies a threshold for inbound ICMP packets. If the number of inbound ICMP packets matched to one single IP address per second exceeds the threshold, system will identify the traffic as an ICMP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. • Action - Specifies an action for ICMP flood attacks. If the default action Drop is selected, system will only permit the specified number (threshold) of IMCP packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period.
	UDP Flood: Click this button to enable UDP flood defense for the security zone. • Src threshold - Specifies a threshold for outbound UDP

Option	Description
	packets. If the number of outbound UDP packets originating from one single source IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. • Dst threshold - Specifies a threshold for inbound UDP packets. If the number of inbound UDP packets destined to one single port of one single destination IP address per second exceeds the threshold, system will identify the traffic as a UDP flood and take the specified action. The value range is 1 to 50000. The default value is 1500. • Action - Specifies an action for UDP flood attacks. If the default action Drop is selected, system will only permit the specified number (threshold) of UDP packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. • Session State Check - Select this check box to enable the function of session state check. After the function is enabled, system will not check whether there is UDP Flood attack in the backward traffic of UDP packet of the identified sessions.
	DNS Query Flood: Click this button to enable DNS query flood defense for the security zone.

Option	Description
	• Src threshold - Specifies a threshold for outbound DNS query packets. If the number of outbound DNS query packets originating from one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. • Dst threshold - Specifies a threshold for inbound DNS query packets. If the number of inbound DNS query packets matched to one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. • Action - Specifies an action for DNS query flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if Alarm is selected, StoneOS will give an alarm but still permit the DNS query packets to pass through.
	Recursive DNS Query Flood: Click this button to enable recursive DNS query flood defense for the security zone. • Src threshold - Specifies a threshold for outbound recursive DNS query packets packets. If the number of outbound DNS query packets originating from one single IP address per second exceeds the threshold, StoneOS will

Option	Description
	identify the traffic as a DNS query flood and take the specified action. • Dst threshold - Specifies a threshold for inbound recursive DNS query packets packets. If the number of inbound DNS query packets destined to one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. • Action - Specifies an action for recursive DNS query flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of recursive DNS query packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if Alarm is selected, StoneOS will give an alarm but still permit the recursive DNS query packets to pass through.
	SYN Flood: Select this check box to enable SYN flood defense for the security zone. • Src threshold - Specifies a threshold for outbound SYN packets (ignoring the destination IP address and port number). If the number of outbound SYN packets originating from one single source IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is

Option	Description

	1500. The value of 0 indicates the Src threshold is void.
	• Dst threshold - Specifies a threshold for inbound SYN packets destined to one single destination IP address per second.
	  • IP-based - Click IP-based and then type a threshold value into the box behind. If the number of inbound SYN packets matched to one single destination IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Dst threshold is void.
	  • Port-based - Click Port-based and then type a threshold value into the box behind. If the number of inbound SYN packets matched to one single destination port of the destination IP address per second exceeds the threshold, StoneOS will identify the traffic as a SYN flood. The value range is 0 to 50000. The default value is 1500. The value of 0 indicates the Dst threshold is void. After clicking Port-based, you also need to type an address into or select an IP Address or Address entry from the Dst address combo box to enable port-based SYN flood defense for the specified segment. The SYN flood attack defense for other segments will be IP based.

Option	Description
	The value range for the mask of the Dst address is 24 to 32. • Action - Specifies an action for SYN flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of SYN packets to pass through during the current and the next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period. Besides if Src threshold and Dst threshold are also configured, StoneOS will first detect if the traffic is a destination SYN flood attack: if so, StoneOS will drop the packets and give an alarm, if not, StoneOS will continue to detect if the traffic is a source SYN attack.
	DNS Reply Flood: Click this button to enable DNS reply flood defense for the security zone. • Src threshold - Specifies a threshold for outbound DNS reply packets. If the number of outbound DNS reply packets originating from one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS query flood and take the specified action. • Dst threshold - Specifies a threshold for inbound DNS reply packets. If the number of inbound DNS reply packets matched to one single IP address per second exceeds the threshold, StoneOS will identify the traffic as a DNS

Option	Description
	reply flood and take the specified action. • Action - Specifies an action for DNS reply flood attacks. If the default action Drop is selected, StoneOS will only permit the specified number (threshold) of DNS reply packets to pass through during the current and next second, and also give an alarm. All the excessive packets of the same type will be dropped during this period; if Alarm is selected, StoneOS will give an alarm but still permit the DNS reply packets to pass through.
	SIP Flood: Click this button to enable SIP flood defense for the security zone. • Dst threshold - Specifies the threshold of the number of the SIP INVITE messages with the same destination IP to be received by the device. That is to say, the device determines that it is attacked by the SIP flood attack when it receives more SIP INVITE messages with the same destination IP than the configured threshold. In this scenario, the device takes further measures to deal with this attack. • Action - Specifies the action of the system when it is attacked by the SIP flood attack. When the system detects the attack, it inspects whether there is a real SIP client behind the subsequent source IP address. If yes, the system bypasses the subsequent SIP INVITE messages sent by this source IP. Otherwise, the system will perform the

Option	Description
	configured action for the SIP INVITE messages sent by this source IP in three seconds. There are two system actions: Drop or Alarm. The action of Drop is the default action and it means dropping the INVITE messages. The action of Alarm means that the system sends an alarm but still bypasses the INVITE messages.
ARP Spoofing	Click the ▶ button to expand the information of the ARP spoofing. Select the **ARP Spoofing** check box to enable all ARP spoofing defenses.
	Max IP number per MAC: Click this button to check the max IP number per MAC. Specifies whether system will check the IP number per MAC in the ARP table. If the parameter is set to 0, system will not check the IP number; if it is set to a value other than 0, system will check the IP number, and if the IP number per MAC is larger than the parameter value, system will take the specified action. The value range is 0 to 1024.
	ARP Send Rate: Click this button to check the ARP send rate. Specifies if StoneOS will send gratuitous ARP packet(s). If the parameter is set to 0 (the default value), StoneOS will not send any gratuitous ARP packet; if it is set to a value other than 0, StoneOS will send gratuitous ARP packet(s), and the number sent per second is the specified parameter value. The value range is 0 to 10.

Option	Description
	Reverse Query: Click this button to enable Reverse query. Select this check box to enable Reverse query. When StoneOS receives an ARP request, it will log the IP address and reply with another ARP request; and then StoneOS will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ARP request packet.
ND Spoofing	**Max IP number per MAC**: Click this button to check the max IP number per MAC. Specifies whether system will check the IP number per MAC in the ND table. System will check the IP number, and if the IP number per MAC is larger than the parameter value, system will take the specified action. The value range is 1 to 1024. **ND Send Rate**: Click this button to check the ND send rate. Specifies if StoneOS will send gratuitous ND packet(s). StoneOS will send gratuitous ND packet(s), and the number sent per second is the specified parameter value. The value range is 1 to 10. **Reverse Query**: Click this button to enable Reverse query. Select this check box to enable Reverse query. When StoneOS receives a NS/NA packet, it will log the IP address and reply with another NS/NA packet; and then StoneOS will check if any packet with a different MAC address will be returned, or if the MAC address of the returned packet is the same as that of the ND packet.

Option	Description
MS-Windows Defense	Click the ▶ button to expand the information of MS-Windows defense. Select the **MS-Windows Defense** check box to enable MS-Windows defense.
	Win Nuke Attack: Click this button to enable WinNuke attack defense for the security zone. If any WinNuke attack has been detected, system will drop the packets and give an alarm.
Scan/Spoof Defense	Click the ▶ button to expand the information of Scan/Spoof Defense. Select the **Scan/Spoof Defense** check box to enable all scan/spoof defenses. **IP Address Spoof**: Click this button to enable IP address spoof defense for the security zone. If any IP address spoof attack has been detected, StoneOS will drop the packets and give an alarm. **ICMP Redirect**: Click this button to enable ICMP redirect attack defense. • Action - Specifies an action for ICMP redirect attacks. If the default action Drop is selected, StoneOS will send an alarm and drop ICMP redirect messages. If the action Alarm is selected, StoneOS will send an alarm but still allow ICMP redirect messages to pass through. **IP Address Sweep**: Click this button to enable IP address sweep defense for the security zone. • Threshold - Specifies a time threshold for IP address sweep. If over 10 ICMP/TCP packets from the same

Option	Description

	source IP address are sent to different hosts within the specified time threshold, StoneOS will identify them as an IP address sweep attack. The value range is 1 to 1,800,000 milliseconds. The default value is 2.
	• Action - Specifies an action for IP address sweep attacks.
	  • Drop: The system will only permit 10 IMCP/TCP packets originating from one single source IP address while matched to different hosts to pass through during the specified period (threshold), and also give an alarm. All the excessive packets of the same type will be dropped during this period. This is the default action.
	  • Block: The system will add the source IP addresses detected within the specified period (threshold) to the blacklist and block the data packets that are sent from the source IP addresses.
	  • Alarm: The system will permit 10 IMCP/TCP packets originating from one single source IP address while matched to different hosts to pass through during the specified period (threshold). For the excessive packets, the system will send an alarm but still allow them to pass through.
	• Block Type- This parameter is available if you set the

Option	Description
	action to Block. You can select Permanent Block or Block Time. By default, Permanent Block is selected. • Permanent Block- The system will permanently block data packets sent from the source IP addresses. • Block Time- Block data packets sent from the source IP addresses within a specified period. Valid values: 1 minute to 15 days. **IP Protocol Scan**: Click this button to enable IP protocol Scan defense for the security zone. • Threshold - Specifies a time threshold for IP protocol scan. If over 10 packets of the same IP protocol from the same source IP address are sent to the same host within the specified time threshold, StoneOS will identify them as an IP protocol scan attack. The value range is 1 to 1,800,000 milliseconds. The default value is 10. • Action - Specifies an action for IP protocol scan attacks. • Drop: The system will only permit 10 packets of the same IP protocol originating from one single source IP address while matched to the same host to pass through during the specified period (threshold) and drop other IP protocol packets, and also give an alarm. This is the default action.

Option	Description
	• Block: The system will add the source IP addresses detected within the specified period (threshold) to the blacklist and block the data packets that are sent from the source IP addresses. • Alarm: The system will permit 10 packets of the same IP protocol originating from one single source IP address while matched to the same host to pass through during the specified period (threshold). For the excessive packets, the system will send an alarm but still allow them to pass through. • Block Type- This parameter is available if you set the action to Block. You can select Permanent Block or Block Time. By default, Permanent Block is selected. • Permanent Block- The system will permanently block data packets sent from the source IP addresses. • Block Time- Block data packets sent from the source IP addresses within a specified period. Valid values: 1 minute to 15 days. **TCP Port Scan**: Click this button to enable port scan defense for the security zone. • Threshold - Specifies a time threshold for port scan. If over 10 TCP SYN packets are sent from the same source

Option	Description

	IP address to different ports within the period specified by the threshold, StoneOS will identify them as a TCP port scan attack. The value range is 1 to 1,800,000 milliseconds. The default value is 5.
	• Action- Specifies an action for TCP port scan attacks.
	  • Drop: During the specified period (threshold), the system will only permit 10 TCP SYN packets destined to different ports to pass through and drops the other packets of the same type, and also generates an alarm.
	  • Block: The system will add the source IP addresses detected within the specified period (threshold) to the blacklist and block the TCP SYN packets that are sent from the source IP addresses to different ports.
	  • Alarm: The system will permit 10 TCP SYN packets destined to different ports to pass through during the specified period (threshold). For the excessive packets, the system will send an alarm but still allow them to pass through.
	• Block Type- This parameter is available if you set the action to Block. You can select Permanent Block or Block Time. By default, Permanent Block is selected.

Option	Description
	• Permanent Block- The system will permanently block data packets sent from the source IP addresses. • Block Time- Block data packets sent from the source IP addresses within a specified period. Valid values: 1 minute to 15 days. **UDP Port Scan**: Click this button to enable UDP Port Scan defense for the security zone. • Threshold - Specifies a time threshold for UDP port scan. If over 10 UDP packets from the same source IP address are sent to different ports within the specified time threshold, StoneOS will identify them as a UDP port scan attack. The value range is 1 to 1,800,000 milliseconds. The default value is 5. • Action- Specifies an action for UDP port scan attacks. • Drop: During the specified period (threshold), the system will only permit 10 UDP packets destined to different ports to pass through and drops the other packets of the same type, and also generates an alarm. • Block: The system will add the source IP addresses detected within the specified period (threshold) to the blacklist and block the UDP packets that are sent from the source IP addresses to different ports.

Option	Description

	• Alarm: The system will permit 10 UDP packets destined to different ports to pass through during the specified period (threshold). For the excessive packets, the system will send an alarm but still allow them to pass through.
	• Block Type- This parameter is available if you set the action to Block. You can select Permanent Block or Block Time. By default, Permanent Block is selected.
	  • Permanent Block- The system will permanently block data packets sent from the source IP addresses.
	  • Block Time- Block data packets sent from the source IP addresses within a specified period. Valid values: 1 minute to 15 days.

Denial of Service Defense	Click the ▶ button to expand the information of denial of service defense. Select the **Denial of Service Defense** check box to enable all denial of service defenses.
	Ping of Death Attack:Click this button to enable Ping of Death attack defense for the security zone. If any Ping of Death attack has been attacked, StoneOS will drop the attacking packets, and also give an alarm.
	Teardrop Attack: Click this button to enable Teardrop attack defense for the security zone. If any Teardrop attack has been attacked, StoneOS will drop the attacking packets, and also give

Option	Description
	an alarm.

Option	Description
	IP Fragment: Click this button to enable IP fragment defense for the security zone. • Action - Specifies an action for IP fragment attacks. The default action is Drop.
	IP Option: Click this button to enable IP option attack defense for the security zone. StoneOS will defend against the following types of IP options: Security, Loose Source Route, Record Route, Stream ID, Strict Source Route and Timestamp. • Action - Specifies an action for IP option attacks. The default action is Drop.
	IP Broadcast Attack: Click this button to enable Smurf or fragile attack defense for the security zone. • Action - Specifies an action for Smurf or fragile attacks. The default action is Drop.
	Land Attack: Click this button to enable Land attack defense for the security zone. • Action - Specifies an action for Land attacks. The default action is Drop.
	Large ICMP Packet: Click this button to enable large ICMP packet defense for the security zone. • Threshold - Specifies a size threshold for ICMP packets. If the size of any inbound ICMP packet is larger than the threshold, StoneOS will identify it as a large ICMP packet

Option	Description
	and take the specified action. The value range is 1 to 50000 bytes. The default value is 1024. • Action - Specifies an action for large ICMP packet attacks. The default action is Drop.
Proxy	Click the ▶ button to expand the information of proxy defense. Select the **Proxy** check box to enable all proxy defenses. **SYN Proxy**: Click this button to enable SYN proxy for the security zone. SYN proxy is designed to defend against SYN flood attacks in combination with SYN flood defense. When both SYN flood defense and SYN proxy are enabled, SYN proxy will act on the packets that have already passed detections for SYN flood attacks. • Proxy trigger rate - Specifies a min number for SYN packets that will trigger SYN proxy or SYN-Cookie (if the Cookie check box is selected). If the number of inbound SYN packets matched to one single port of one single destination IP address per second exceeds the specified value, StoneOS will trigger SYN proxy or SYN-Cookie. The value range is 1 to 50000. The default value is 1000. • Cookie - Select this check box to enable SYN-Cookie. SYN-Cookie is a stateless SYN proxy mechanism that enables StoneOS to enhance its capacity of processing multiple SYN packets. Therefore, you are advised to expand the range between "Proxy trigger rate" and "Max SYN

Option	Description
	packet rate" appropriately. • Max SYN packet rate - Specifies a max number for SYN packets that are permitted to pass through per second by SYN proxy or SYN-Cookie (if the Cookie check box is selected). If the number of inbound SYN packets destined to one single port of one single destination IP address per second exceeds the specified value, StoneOS will only permit the specified number of SYN packets to pass through during the current and the next second. All the excessive packets of the same type will be dropped during this period. The value range is 1 to 1500000. The default value is 3000. • Timeout - Specifies a timeout for half-open connections. The half-open connections will be dropped after timeout. The value range is 1 to 180 seconds. The default value is 30.
Protocol Anomaly Report	Click the ▶ button to expand the information of protocol anomaly report. Select the **Protocol Anomaly Report** check box to enable the function of all protocol anomaly reports. **TCP Anomalies**: Click this button to enable TCP option anomaly defense for the security zone. • Action - Specifies an action for TCP option anomaly attacks. The default action is Drop. **TCP Split Handshake**: Click this button to enable TCP split

Option	Description
	handshake defense for the security zone. • Action - Specifies an action for TCP split handshake attacks. The default action is Drop.



Notes:

In Tap zone, you cannot set the action to Block for IP address sweep, IP protocol scan, TCP port scan, UDP port scan in scan/spoof defense.

4. To restore the system default settings, click **Restore Default**.
5. Click **OK**.

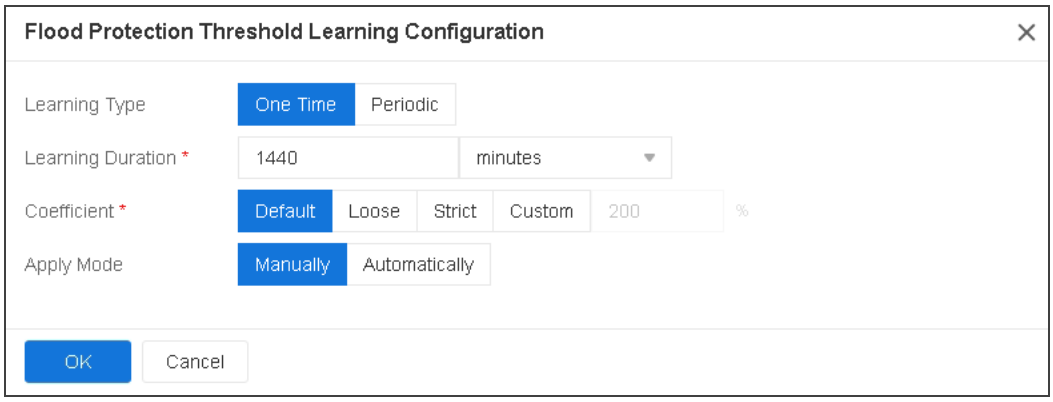
Configuring Flood Protection Threshold Learning

Configuring Flood Protection Threshold Learning Parameters

To configure flood protection threshold learning parameters, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. On the **Zone Configuration** page, expand **Threat Protection**.
3. Click the **Enable** button next to **Attack Defense** and then **Configure**.

4. In the **Attack Defense** panel, click **Configure** next to **Flood Protection Threshold Learning**.



Option	Description
Learning Type	Specifies the type of flood protection threshold learning. Valid values: One Time and Periodic. Default value: One Time. One Time: Runs the learning task only once, which will be automatically stopped after completion. Periodic: Runs the learning task periodically based on the interval. You need to manually stop the learning task. If you set the type to this value, you also need to specify the periodic interval. • Periodic Interval: This value specifies the interval between the last time when the learning task ends and the next time when the learning task starts. To specify an interval, enter a time period in the field and select a time unit from the drop-down list. Valid units: minutes, hours, and days. • If the time unit is set to days, valid values of the interval are 1 to 365 days and the default value is 7 days.

Option	Description
	• If the time unit is set to hours, valid values of the interval are 1 to 8760 hours and the default value is 1 hour. • If the time unit is set to minutes, valid values of the interval are 10 to 525600 minutes and the default value is 1440 minutes.
Learning Duration	Specifies the duration of flood protection threshold learning. To do this, enter a time period in the field and select a time unit from the drop-down list. Valid units: minutes, hours, and days. • If the time unit is set to days, valid values of the duration are 1 to 365 days and the default value is 1 day. • If the time unit is set to hours, valid values of the duration are 1 to 8760 hours and the default value is 1 hour. • If the time unit is set to minutes, valid values of the duration are 10 to 525600 minutes and the default value is 1440 minutes.
Coefficient	Final threshold learning result=Maximum traffic rate within learning duration * Coefficient. Specifies the coefficient of flood protection threshold learning. Unit: %. You can select Default, Loose, Strict, or customize a coefficient. • Default: The coefficient is 200. • Loose: The coefficient is 4000. • Strict: The coefficient is 100.

Option	Description
	• Custom: The coefficient range is from 100 to 4000.
Apply Mode	Specifies the mode of applying the flood protection threshold learning result. Valid values: Manually and Automatically. Default value: Manually. • Manually: Applies the threshold learning result to the threshold configuration of a flood attack defense item based on your requirements. For more information, see Viewing and Applying Flood Protection Threshold Learning Result. • Automatically: The threshold configuration of all enabled flood attack defense items will be automatically configured with the threshold learning result and these threshold configurations will be automatically applied.

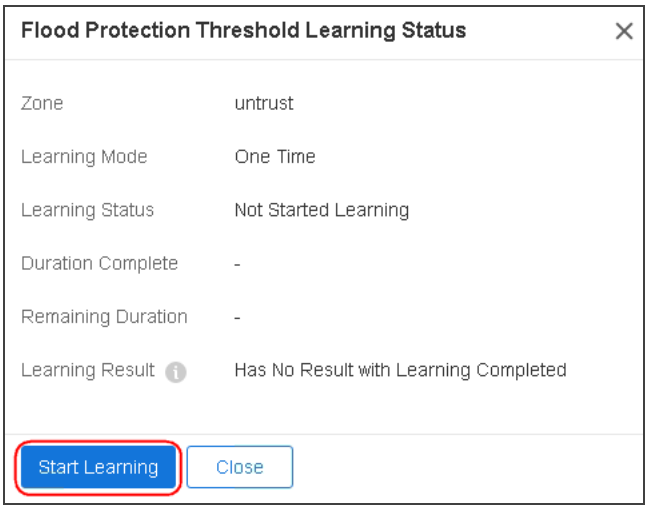
5. Click **OK**.

Enabling Flood Protection Threshold Learning

After you configure flood protection threshold learning parameters, you can start flood protection threshold learning. To do this, take the following steps:

1. Select **Network** > **Zone**.
2. In the list of zones whose Attack Defense function is enabled, click **Status** in the **AD Intelligent Learning** column. In the **Flood Protection Threshold Learning Status** panel, click

Start Learning.



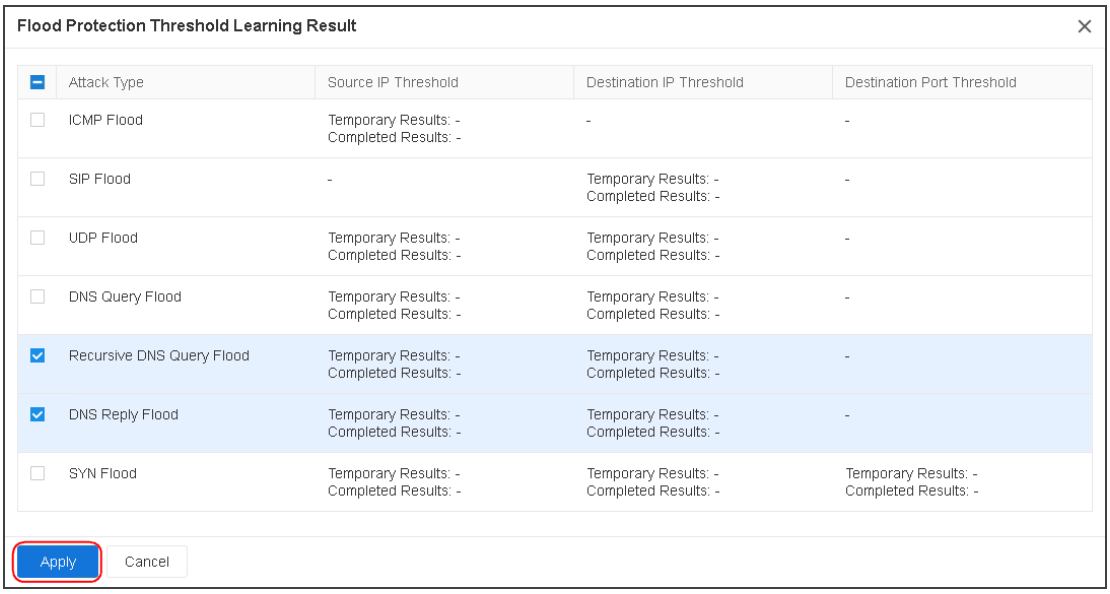
3. After flood protection threshold learning is started, you can view details such as the duration completed, remaining duration, and learning result. You can also click Stop Learning to stop flood protection threshold learning.

Viewing and Applying Flood Protection Threshold Learning Result

After flood protection threshold learning is completed, you can view and apply the learning result. To do this, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. On the **Zone Configuration** page, expand **Threat Protection**.
3. Click the **Enable** button next to **Attack Defense** and then **Configure**.
4. Click **View Result** next to **Flood Protection Threshold Learning**. In the **Flood Protection Threshold Learning Result** panel, view threshold learning result of each flood attack type, including completed results and temporary results. To use a temporary result, you need to record this result and manually replace the threshold of the corresponding flood attack

defense item with this result.



5. Select the flood attack type whose threshold learning result you want to apply and click **Apply**.

Notes:

- The Flood Protection Threshold Learning function takes effect only if the Attack Defense function and corresponding flood attack defense items are enabled.
- Flood protection threshold learning parameters cannot be edited when flood protection threshold learning is in progress.
- The minimum value of actual flood protection threshold learning result is 1500 and the maximum value is consistent with that of the flood attack defense item you can configure.
- In HA state, only the master device can perform flood protection threshold learning. After the master device starts learning, the learning result is not

synchronized to the backup device. The threshold configuration is synchronized to the backup device only after the learning result is applied to the master device. If a switchover occurs, threshold learning automatically stops.

- If the device is restarted, you need to start flood protection threshold learning again.

Antispam

SG-6000-A200 and SG-6000-A200W do not support this function.

The system is designed with an Antispam function, which enables user to identify and filter mails transmitted by SMTP and POP3 protocol through the cloud server, timely discover the mail threats, such as spam, phishing and worm mail, and then process the found spam according to the configuration, so as to protect the user's mail client or mail server.

Notes: The Antispam function will not work unless an Antispam license has been installed on a StoneOS that supports Antisspam.

Related Topics:

- "Configuring Antispam" on Page 1422
- "Antispam Global Configuration" on Page 1428

Configuring Antispam

This chapter includes the following sections:

- Preparation for configuring Antispam function
- Configuring Antispam function

Preparing

Before enabling Antispam, make the following preparations:

1. Make sure your system version supports Antispam.
2. Import an Antispam license and reboot. The Antispam will be enabled after the rebooting.



Notes: To assure a proper connection to the cloud server, you need to configure a DNS server for StoneOS before configuring the anti-spam.

Configuring Antispam Function

The Antispam configurations are based on security zones or policies.

- If a security zone is configured with the Antispam function, system will perform detection on the traffic that is matched to the binding zone specified in the rule, and then do according to what you specified.
- If a policy rule is configured with the threat protection function, system will perform detection on the traffic that is matched to the policy rule you specified, and then respond.
- The threat protection configurations in a policy rule is superior to that in a zone rule if specified at the same time, and the threat protection configurations in a destination zone is superior to that in a source zone if specified at the same time.

To realize the zone-based Antispam, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. In the Zone Configuration page, expand Threat Protection.

3. Enable the threat protection you need and select an Anti-Spam rule from the profile drop-down list below; or you can click ⊕ from the profile drop-down list. To create an Anti-Spam rule, see Configuring an Anti-Spam Rule.

4. Click **OK** to save the settings.

To realize the zone-based Antispam, take the following steps:

1. Create a security policy rule. For more information, refer to "Security Policy" on Page 1089.

2. In the Policy Configuration page, expand the Protection.

3. Click the **Enable** button of **Antispam**. Then select an Antispam rule from the Profile drop-down list, or you can click ⊕ from the Profile drop-down list to create an Anti-Spam rule. For more information, see Configuring an Anti-spam Rule.

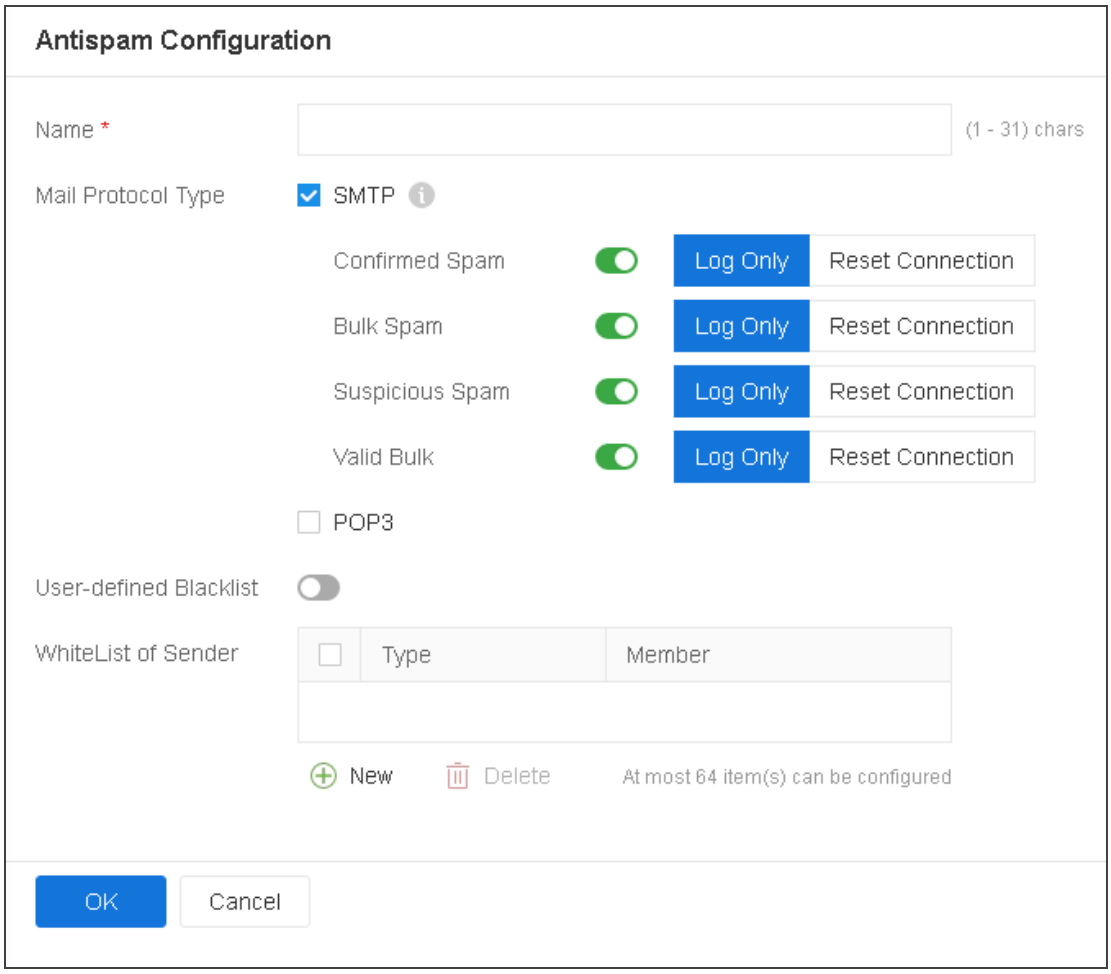
4. Click **OK** to save the settings.

Configuring an Antispam Rule

To configure an Antispam rule, take the following steps:

1. Select **Object > Antispam > Profile**.

2. Click **New**



Option	Description
Name	Specifies the rule name.
Mail Protocol Type	Specifies the mail protocol (SMTP, POP3), spam category and action.spam category: • Confirmed Spam: The mail from spam source. • Bulk Spam: The malicious mass mail from uncertain spam sources.

Option	Description
	• Suspicious Spam: The mail from suspicious spam sources. • Valid Bulk: Mass mail from legitimate senders. Action: • Log Only - Only generates log. This is the default action. • Reset Connection - If spams has been detected, system will reset connections. **Note**: The spams transferred over POP3 only supports generate logs action.
User-defined Blacklist	Click the **Enable** button to enable the Antispam User-defined Blacklist. When it is enabled, the email from the sender who is in the User-defined Blacklist will be directly identified as spam, and then system will process it according to the action specified by users, log or reset connection.
Whitelist of Sender	The whitelist is used to specify the mail domains or email that will not be filtered by Anti-Spam. Each Anti-Spam profile can specify up to 64 whitelist items. • Select "Domain " or "Email " and enter the corresponding parameter values in the text box. The parameter values range from 1 to 255 characters. When "Domain" is selected, the maximum length between the two periods (.) is only 63 characters.

Option	Description
	• Click **New** to add the domain name or email address to whitelist of sender. • Select the domain or email address of sender item, and click **Delete**to delete the items of sender.

3. Click **OK**.

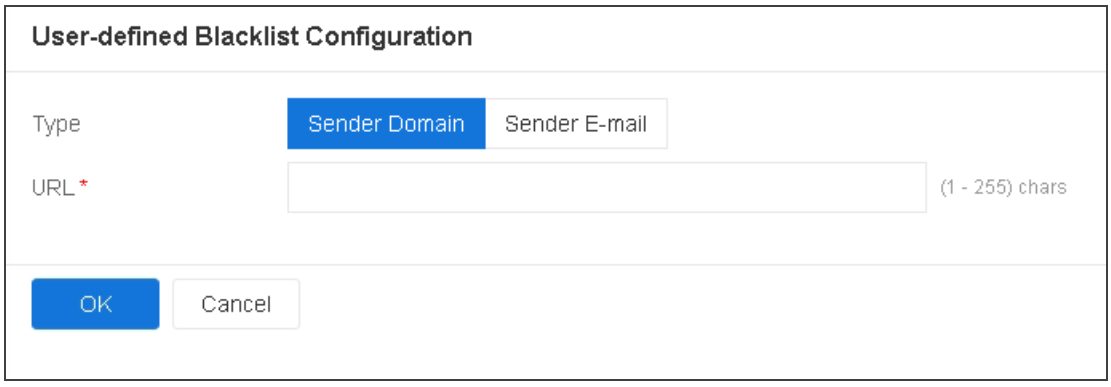
Notes: By default, system comes with one default spams filtering rules: predef_ default. The default rule is not allowed to edit or delete.

Configuring an Anti-Spam User-defined Blacklist

You can add the sender's domain name or email address to the User-defined Blacklist. When Anti-Spam User-defined Blacklist function is enabled, system will directly identify the email from the User-defined Blacklist as spam, and reset the link or record to the threat log.

To configure an Anti-Spam User-defined Blacklist, take the following steps:

1. Select **Object > Antispam > User-defined Blacklist** and click **New**.



2. In < User-defined Blacklist Configuration > page, select "Sender Domain " or "Sender E-mail " and enter the corresponding parameter values in the text box. The parameter values

range from 1 to 255 characters. When "Sender Domain" is selected, the maximum length between the two periods (.) is only 63 characters.

3. Click **OK**.

To export the sender User-defined Blacklist, take the following steps:

1. Select **Object > Antispam > User-defined Blacklist**.
2. Click **Export** and all the item of the User-defined Blacklist will be exported as an file in the format of ".txt ".

The exported User-defined Blacklists can be imported on another device. To import the sender User-defined Blacklist, take the following steps:

1. Select **Object> Antispam > User-defined Blacklist** and click **Import**.
2. In the<Import User-defined Blacklist> page, click the **Browse** to select the User-defined Blacklist file to be imported.
3. Click **OK** to import User-defined Blacklist .

Notes: If you import a new anti-spam blacklist, all the existing user-defined anti-spam blacklists are replaced. To retain the existing user-defined anti-spam blacklists, export and merge them with the new one, and then import the merged result.

Antispam Global Configuration

To configure the Antispam global settings, take the following steps:

1. Click **Object** > **Antispam** > **Configuration**.



2. Type in the mail scan maximum limit in the **Mail Scan Upper Limit** text box. The range is 512 Kb to 2048 Kb, the default value is 1024 Kb.

3. Click **OK** to save the settings.

Botnet Prevention

Botnet refers to a kind of network that uses one or more means of communication to infect a large number of hosts with bots, forming a one-to-many controlled network between the controller and the infected host, which will cause a great threat to network and data security.

The botnet prevention function can detect botnet host in the internal network timely, as well as locate and take other actions according to the configuration, so as to avoid further threat attacks.

The botnet prevention configurations are based on security zones or policies. If the botnet prevention profile is bound to a security zone, the system will detect the traffic destined to the specified security zone based on the profile configuration. If the botnet prevention profile is bound to a policy rule, the system will detect the traffic matched to the specified policy rule based on the profile configuration.

DGA Detection

DNS as the domain name resolution protocol, is designed to resolve fixed domain names to IP addresses. Due to the use of domain name is convenient, and is widely used, so the attacker will take different means to use the domain name to generate attack. For example, A IP address can correspond to multiple domain name, the server according to the endpoint field of HTTP packet to find the Goal URL, the malware will use this feature by modifying the endpoint field to

disguise the domain name, and generate the abnormal behavior. DGA, is the domain generation algorithm, this algorithm will generate a large number of pseudo random domain name, and will be used by malware.

To solve these problem, system supports to enable DGA detection function to detect DNS response messages and detect whether the device is attacked by DGA domain name. If a DGA domain name is detected, the system will perform the specified processing actions on the detected DGA domain name according to the configuration of the botnet prevention rules (record the related threat log, reset the connection, or replace the sinkhole).

DNS Tunnel Detection

DNS tunnel is a kind of covert channel, which establishes communication by encapsulating other protocols in DNS protocol for transmission. However, most firewalls and detection devices release DNS traffic, and DNS tunnel attacks formally use the features of the release to implement operations such as remote control and file transfer, which cause harm to users' network security and data security. Therefore, the detection, warning, and processing of DNS tunnels are particularly important.

System provides the DNS tunnel detection function. Through the detection of DNS request messages and the monitoring of DNS traffic, the feature extraction and comprehensive analysis of the DNS tunnel can be realized. At the same time, the specified processing action can be performed on the detected DNS tunnel (Record the relevant threat log or reset the connection) to prevent the threat brought by the DNS tunnel.



Notes: The botnet prevention function is controlled by license. DGA detection and DNS tunnel detection are included in the botnet prevention function. Therefore, botnet prevention, DGA detection, and DNS tunnel detection can be used only after the Botnet Prevention license is installed in StoneOS.

Related Topics:

- "Configuring Botnet Prevention" on Page 1431
- "Address Library" on Page 1435
- "Botnet Prevention Global Configuration" on Page 1446

Configuring Botnet Prevention

This chapter includes the following sections:

- Preparation for configuring Botnet Prevention function
- Configuring Botnet Prevention function

Preparing

Before enabling botnet prevention, make the following preparations:

1. Make sure your system version supports botnet prevention.
2. Import a botnet prevention license and reboot. The botnet prevention will be enabled after the rebooting.



Notes:

- You need to update the botnet prevention signature database before enabling the function for the first time. To assure a proper connection to the default update server, you need to configure a DNS server for system before updating.

Configuring Botnet Prevention Function

The Botnet Prevention configurations are based on security zones or policies.

To realize the zone-based Botnet Prevention, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. In the Zone Configuration page, expand Threat Protection.
3. Enable the threat protection you need and select a Botnet Prevention rule from the profile drop-down list below; or you can click ⊕ from the profile drop-down list. To create a Botnet Prevention rule, see Configuring a Botnet Prevention Rule.
4. Click **OK** to save the settings.

To realize the zone-based Botnet Prevention, take the following steps:

1. Create a security policy rule. For more information, refer to "Security Policy" on Page 1089.
2. In the Policy Configuration page, expand the Protection.
3. Click the **Enable** button of **Botnet Prevention**. Then select an Anti-Spam rule from the Profile drop-down list, or you can click ⊕ from the Profile drop-down list to create a Botnet Prevention rule. For more information, see Configuring a Botnet Prevention Rule.
4. Click **OK** to save the settings.

Configuring a Botnet Prevention Rule

You can use default botnet prevention rules or create custom rules. The system provides 3 default botnet prevention rules: predef_critical, predef_default, and no-botnet-c2-prevention.

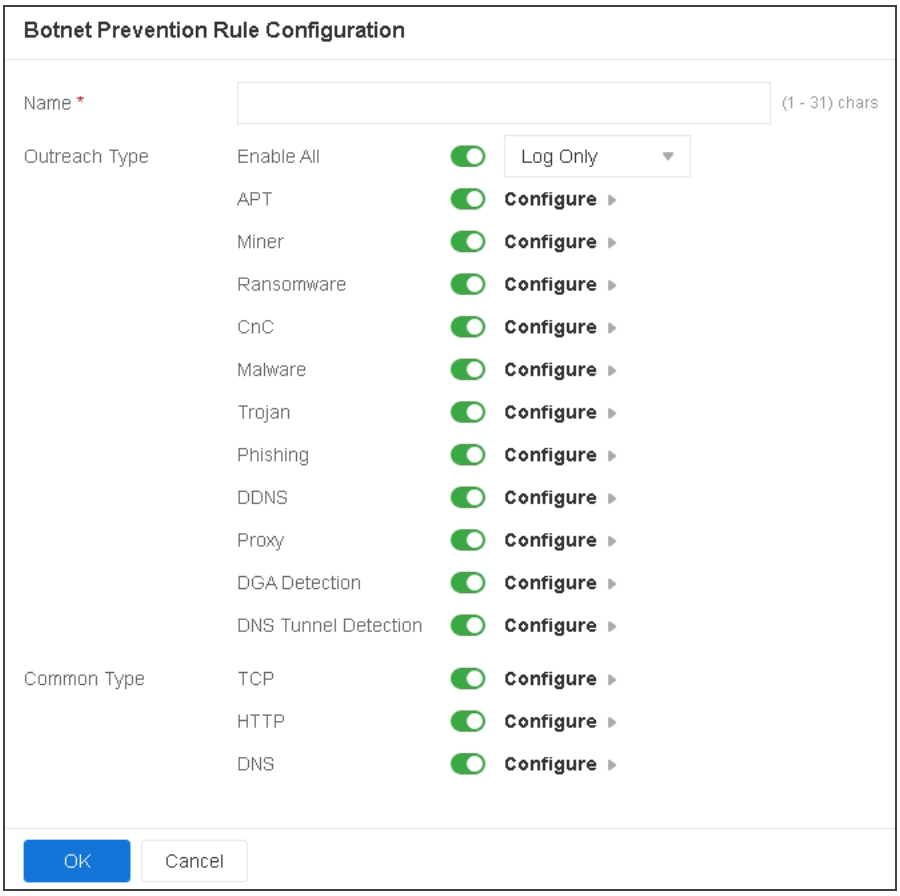
- **predef_critical** - The strict botnet prevention check policy. This rule is used to scan TCP/HTTP/DNS traffic. When a zombie host is detected, malicious connection is reset and threat logs will be recorded.
- **predef_default** - The loose botnet prevention check policy. This rule is used to scan TCP/HTTP/DNS traffic. When a zombie host is detected, traffic is allowed and the system

only records threat logs.

- **no-botnet-c2-prevention** – This rule does not implement any botnet prevention check.

To configure a Botnet Prevention rule, take the following steps:

1. Click **Object** > **Botnet Prevention**> **Profile**.
2. Click **New**.



Option	Description
Name	Specifies the rule name.
Outreach Type	Specifies the outreach type (i.e., IOC tag type) that needs to be protected and specifies the corresponding action. After

Option	Description
	enabled, when traffic hits the predefined/custom blocking list or cloud query cache blacklist, the IOC tag of the traffic data will be detected and processed based on the specified outreach type and the corresponding action; if not enabled, traffic will be detected and processed based on the protocol configuration of the common type. • Enable All: Turn on the switch to enable the protection for all outreach types. Select an action to be taken from the drop-down list. The action can be Log Only or Reset Connection. • Turn on the switch next to a specified outreach type to enable the protection for this type. • Click **Configure** to enable scan of different protocols (TCP, HTTP, DNS) for the selected outreach type and select the corresponding action. • Local Intelligent Algorithm: For the DGA Detection type and DNS Tunnel Detection type, the Local Intelligent Algorithm function is enabled by default. You can use this function to improve the accuracy rate of detection and reduce the false positive rate. Note: • The priority of the outreach type is higher than that of the common type.

Option	Description
	• The priority of each IOC tag type in the outreach type is ranked in ascending order based on the order displayed on the page.
Common Type	Specifies the protocol types (TCP, HTTP, DNS) that the system will scan and specifies the action the system will take after the botnet is found. • Log Only - Only generates log. • Reset Connection - If botnets has been detected, system will reset connections to the files. • Sinkhole-Replace - When the protocol type is DNS, you can specify the processing action as "Sinkhole Address Replacement". After the threat is discovered, the system will replace the IP address in the DNS response packet with the Sinkhole IP address.

3. Click **OK**.

Address Library

The address library contains block list, exclude list, and cloud cache, in which the block list and exclude list includes predefined and custom list. They are described as follows:

- **Exclude list**: When the traffic matches to the IP address, domain name, or URL in the list, system **will not** control the traffic with botnet prevention function. The **predefined exclude list** is obtained automatically through the botnet prevention signature database; the **custom exclude list** contains IPs, domains and URLs manually added by the user

- **Block list**: When the traffic matches to the IP address, domain name or URL in the list, system **will** control the traffic with botnet prevention function. The **predefined block list** is obtained automatically through the botnet prevention signature database; the **custom block list** contains IPs, domains and URLs manually added by the user
- **Cloud Cache**: Displays check results of unknown domains in the cloud in real time, along with domain/IP/URL addresses automatically pushed by the cloud. You can perform precise queries in the cloud cache information based on specified IP/domain/URL and use these results to take corresponding measures.



Notes:

- The traffic matching sequence for the botnet prevention function will be: Custom exclude list > Custom block list > Cloud cache > Predefined exclude list > Predefined block list.
- Entries in the cloud cache are not added to the botnet prevention address library, but only cached in the device.

Exclude List

Creating a Custom Exclude List

To create a custom exclude list entry, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.
2. In the Exclude List tab, click **New** to open the **Exclude Entry Configuration** page.
3. Click **IP**, **Domain** or **URL** to specify the entry type.
    - IP: Enter the IP address and Port in the text box. If not specified the port,it will be any port.

- Domain: Enter the domain name in the text box. You can click the **enable** button of "Including subdomains" to specify the domain as a wildcard domain.
- URL: Select HTTP or HTTPS from the URL drop-down list and enter the URL address in the text box.

4. Click **OK**.

Deleting a Custom Exclude List

To delete a custom exclude list entry, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.
2. In the Exclude List tab, select the entry you want to delete from the exclude list.
3. Click **Delete**.

Filtering a Entry in the Exclude List

Users can filter and view an exclude list entry in the predefined address library and the custom address library. To filter an exclude list entry, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.
2. In the Exclude List tab, click the **Filter** button to add filtering conditions and search out the filtered entry.

Block List

Creating a Custom Block List

To create a custom block list entry, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.
2. In the Block List tab, click **New** to open the **Blocklist Entry Configuration** page.

3. Click **IP**, **Domain** or **URL** to specify the entry type.
    - IP: Enter the IP address and Port in the text box. If not specified the port,it will be any port.
    - Domain: Enter the domain name in the text box. You can click the enable button of "Including subdomains" to specify the domain as a wildcard domain.
4. Click **OK**.

Deleting a Custom Block List

To delete a custom block list entry, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.
2. In the Blick List tab, select the entry you want to delete from the block list.
3. Click **Delete**.

Filtering a Entry in the Block List

Users can filter and view a block list entry in the predefined address library and the custom address library. To filter a block list entry, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.
2. In the Block List tab, click the **Filter** button to add filtering conditions and search out the filtered entry.

Adding to Exclude List

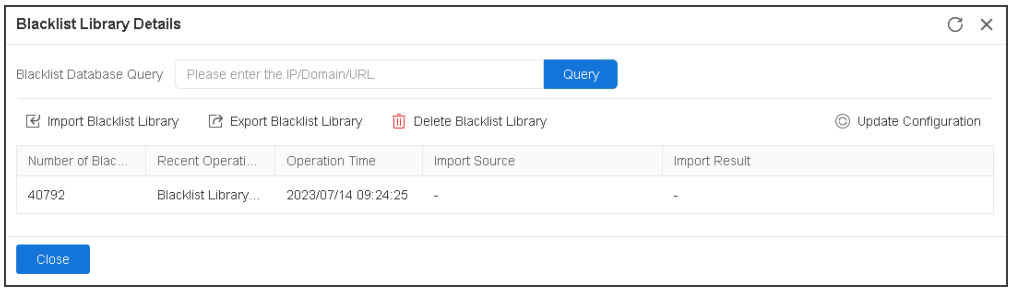
To add a block list entry to the exclude list, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.
2. In the Block List tab, click **Add to exclude list** under the Operation column in the block list to add the entry to the exclude list.

Configuring the Blacklist Library

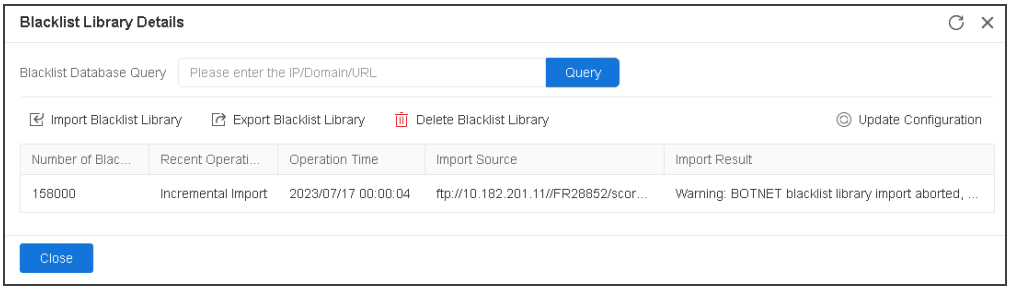
The blacklist library is stored as a file containing a collection of blacklist entries, including IP addresses, domain names, or URLs.

You can manually import/export the blacklist library or automatically update the blacklist library file from a specified server.



To manually import a blacklist library file, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.
2. In the **Block List** tab, click **Blacklist Library Details**.
3. In the **Blacklist Library Details** panel, click **Import Blacklist Library**.



4. Select **Incremental Import** or **Overwrite Import**.
    - Incremental Import: Continue to import a blacklist library file on top of the existing file.
    - Overwrite Import: Overwrite the existing blacklist library file with a new one.

5. In the **File Name** field, click **Browse** and select a file from your PC.

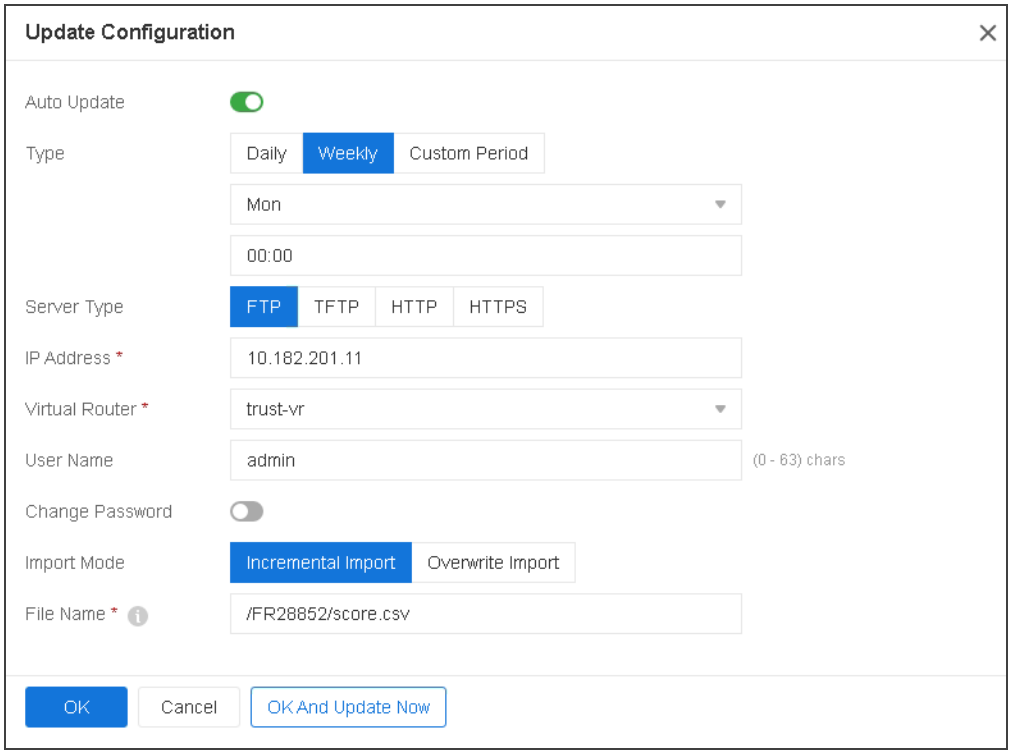
6. Click **OK**.

To configure auto update, take the following steps:

1. Click **Object > Botnet Prevention > Address Library**.

2. In the **Block List** tab, click **Blacklist Library Details**.

3. Click **Update Configuration**.



4. Enable **Auto Update** to automatically update the blacklist library file from the specified server.

Option	Description
Type	Specifies the time interval, including every day, every week, or a custom period.

Option	Description
	• Daily: Automatically updates the file at a specified time every day. You can specify the point in time. Default value: 00:00. Valid values: 00:00 to 23:59. • Weekly: Automatically updates the file at a specified time every week. You can specify the day of the week and then the point in time. Default value: 00:00 on Monday. Valid values: 00:00 on Monday to 23:59 on Sunday. • Custom Period: Automatically updates the file after a custom time period. Valid values: 30 to 10080 minutes.
Server Type	Specifies the server type, including FTP, TFTP, HTTP, or HTTPS.
IP Address	If you set the server type to FTP or TFTP, enter the IP address of the server.
URL	If you set the server type to HTTP or HTTPS, enter the URL of the server in the field. The URL needs to be 1 to 255 characters in length. **Note:** • The URL of the HTTP server needs to start with "http://" and the URL of the HTTPS server needs to start with "https://". • The URL for the HTTP/HTTPS server needs to end with a file name suffix such as .csv, .json, .stix2, .ioc, or .xml. Example: http://192.1.1.1:8080/chf-s/shared/SERVER/ftp/test/score.csv

Option	Description
Virtual Router	Specifies the virtual router of the server.
User Name	If you set the server type to FTP, enter the username used to log on to the FTP server.
Password	If you set the server type to FTP, enter the password of the FTP username. **Change Password**: To change your password, enable **Change Password** when you edit the update configuration. With this function enabled, you can enter a new password. This way, the password corresponding to the username used to log in to the FTP server is changed.
Import Mode	Select the import mode, including incremental import and overwrite import. • Incremental Import: Continue to import a blacklist library file on top of the existing file. • Overwrite Import: Overwrite the existing blacklist library file with a new one.
File Name	If you set the server type to FTP or TFTP, enter the name of the file to be imported.

5. Click **OK**.
6. You can also click **OK And Update Now** to save the settings and update the blacklist library immediately.

Notes:

- The manually imported or automatically updated blacklist library files support the following formats: CSV/STIX/OpenIOC. The file name extension can be .csv/.json/.stix2/.ioc/.xml. For CSV files, the format is as shown in the following example, in which the first column displays the type, including IPv4/domain/URL, and the second column displays the blacklist address of the corresponding type.

Indicator type	Indicator	Description
IPv4	192.168.5.3	
domain	test.com	
URL	http://192.168.5.36/	

- The size of manually imported or automatically updated blacklist library files cannot exceed 100 MB.
- The blacklist library files to be imported or automatically updated will be checked for redundancy in the order of import. If the format and content of the blacklist library file are valid, the import will be successful. The corresponding logs will display the total number of blacklist entries in the imported file, the actual number of imported blacklist entries, and the number of duplicate blacklist entries.
- When manually importing or automatically updating the blacklist library file, if the imported blacklist entries exceed the blacklist and whitelist capacity of botnet prevention of the device, the manual import will fail; In this case, the maximum number of entries that fit within the total blacklist and whitelist capacity of botnet prevention of the device, and the remaining blacklist entries will not be imported.

You can also perform the following operations:

- Export Blacklist Library: Click **Export Blacklist Library** to export blacklist library file to your PC.
- Delete Blacklist Library: Click **Delete Blacklist Library** to delete the blacklist library file.
- Blacklist Database Query: In the search box, enter an IP address, domain, or URL and click **Query** to search for the specified blacklist entry.



Notes:

- The export/delete/query operations can be performed only on the blacklist library, but do not affect the blacklist in the Creating a Custom Block List section.
- SG-6000-A2200, SG-6000-A1800, and SG-6000-A1600 do not support the blacklist library.

Cloud Cache

Before you begin:

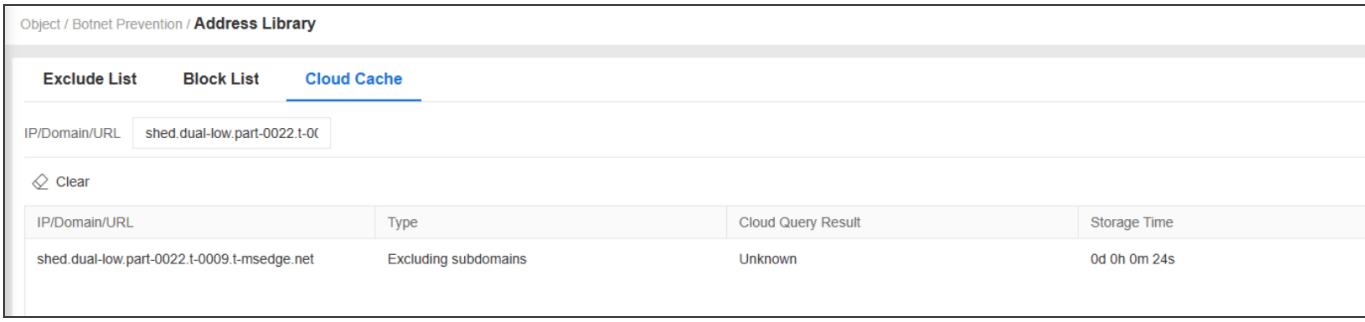
- **Read** "Cloud-Network Collaborative DNS Protection" on Page 1493
- **Read** "Introduction" on Page 1493
- "Configuring Unknown Domain Cloud Collaborative Query" on Page 1494

After the device is connected to the Hillstone cloud platform, the cloud will periodically push domain/IP/URL to the device. This data, along with results from unknown domain cloud queries, is stored in the device's "Cloud Cache" for future threat detection of botnet prevention. You can precisely query detailed cloud query results by specifying an IP/domain/URL on the **Cloud Cache** tab and proceed with relevant operations based on the query results.

Notes: It is essential to use a known and specific domain/IP/URL when performing queries on this tab.

To search for cloud query results by IP/domain/URL, take the following steps:

1. Select **Object** > **Botnet Prevention** > **Address Library**.
2. Click the **Cloud Cache** tab.
3. In the **IP/Domain/URL** search box, enter the precise IP address, domain, or URL, then press Enter. The cache information will display the detailed type, cloud query result, and storage time in the list below.



4. View cloud query results of the unknown domain. Different actions can be taken based on the cloud query results for unknown domains:
   - **Blacklist**: If the **Cloud Query Result** is **Blacklist**, traffic associated with the domain will be processed based on the botnet defense rules configured in the system. If the domain is determined to be a false positive or the traffic is considered safe to allow, the domain can be added to the custom exception list. To do this, click **Add to exclude list** in the **Operation** column. Once added, any traffic matching this IP address, domain, or URL will no longer be controller by the botnet defense function.
   - **Whitelist/Unknown**: If the **Cloud Query Result** is **Whitelist** or **Unknown**, the traffic will be allowed by default.

5. View the storage duration for cached unknown domains. The maximum storage duration is 24 hours. Once a domain in the cloud cache reaches 24 hours, it is automatically deleted from the device.

Clearing All Cloud Cached Data

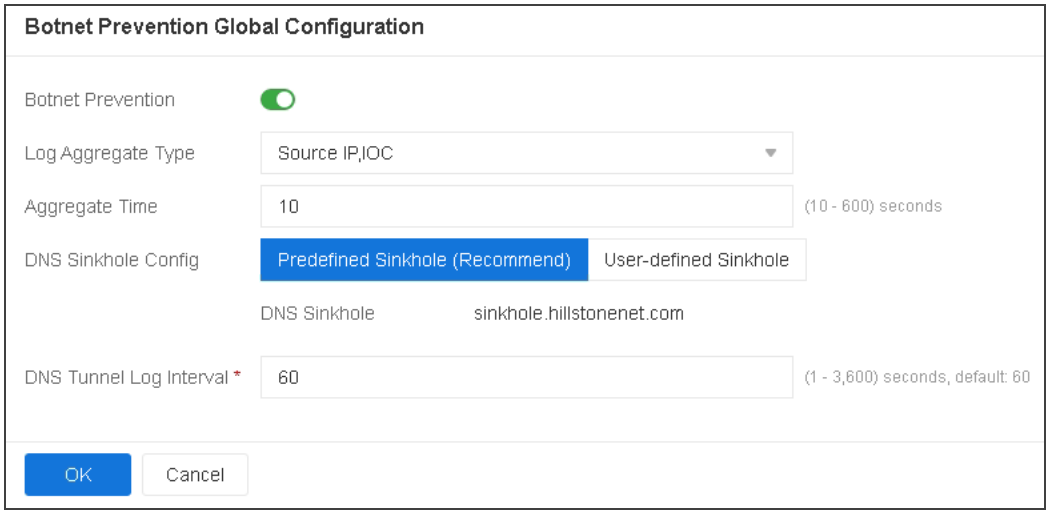
Cloud query cached data is automatically cleared when the device is restarted. In certain scenarios, such as releasing device memory or after a traffic switch, you may need to manually clear all cloud query cached results stored on the device. To do this, take the following steps:

1. Select **Object** > **Botnet Prevention** > **Address Library**.
2. Click the **Cloud Cache** tab.
3. Click **Clear**. In the tips message, click **OK**.

Botnet Prevention Global Configuration

To configure the Botnet Prevention global settings, take the following steps:

1. Click **Object** > **Botnet Prevention** > **Configuration**.



2. Click/clear the **Enable** button to enable/disable the Botnet Prevention function.

3. In the **Log Aggregate Type**section, select the aggregation type for the anti-virus logs. If **Do Not Merge** is not selected, the system will merge botnet prevention logs based on specified log aggregation type and time granularity. This way, logs are reduced to prevent the log server from receiving redundant logs.

   Option descriptions:

Option	Description
Do Not Merge	The system stores each botnet prevention log in the database and does not merge any logs.
Source IP	The system merges botnet prevention logs of the same source IP according to the specified time granularity.
Destination IP	The system merges botnet prevention logs of the same destination IP according to the specified time granularity.
Source IP, Destination IP	The system merges botnet prevention logs of the same source and destination IP according to the specified time granularity.
Source IP, IOC	The system merges botnet prevention logs of the same source IP and IOC according to the specified time granularity. IOC indicates threat intelligence, that is to say, the malicious domain name, IP address, or URL detected by the botnet prevention function.
Destination IP, IOC	The system merges botnet prevention logs of the same destination IP and IOC according to the specified time granularity. IOC indicates threat intelligence, that is to say, the malicious domain name, IP address, or URL detected by the botnet prevention function.
Souce IP,	The system merges botnet prevention logs of the same source

Option	Description
Destination IP, IOC	IP, destination IP, and IOC according to the specified time granularity. IOC indicates threat intelligence, that is to say, the malicious domain name, IP address, or URL detected by the botnet prevention function.

4. In the **Aggregate Time** section, specifies the time granularity for merging botnet prevention logs. With this parameter specified, at the same time granularity, the system stores botnet prevention logs of the same merging type (specified above) in the database only once. Value ranges from 10 to 600 seconds. The default value is 10 seconds.

5. Specify the Sinkhole IP address that replaces the IP address in the DNS response message. You can select the system's predefined Sinkhole IP address or specify a user-defined Sinkhole IP address. After selecting **User-defined Sinkhole**, specify a custom IPv4 address and an IPv6 address. If only the IPv4 address is configured, the system will automatically map the configured IPv4 address to the corresponding IPv6 address when the DNS server communicates by using the IPv6 protocol.

6. In the **DNS Tunnel Log Interval**, specify the minimum time interval for logging after the system detects the DNS tunnel. The range is 1 to 3600 seconds, the default value is 60 seconds.

7. Click **Apply** to apply the settings.

Encrypted Traffic Detection

Traffic processed by using encryption technology is called encrypted traffic. Malicious traffic is typically hidden by using SSL/TLS encryption protocols, which is difficult to detect and can pose great threats to network security. After you configure the Encrypted Traffic Detection function, the system extracts feature data from encrypted traffic and detects the data based on the detection

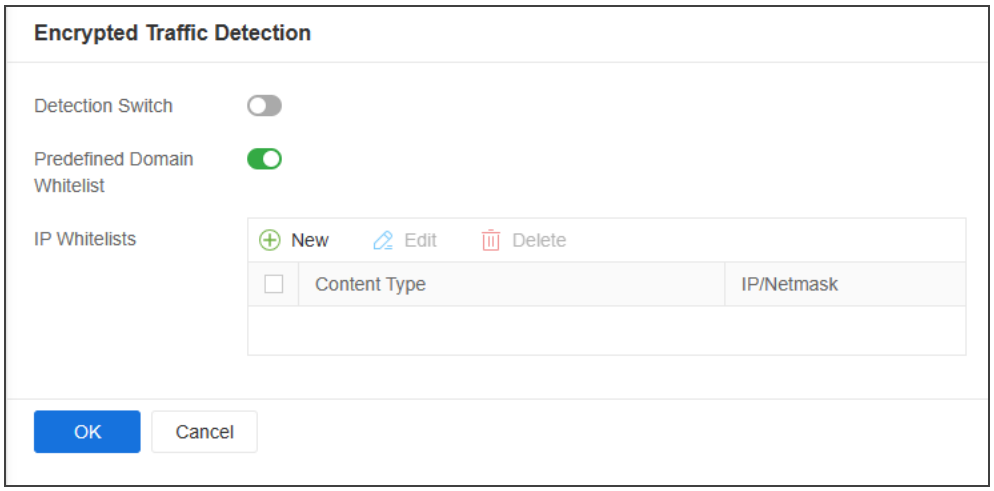
model in the encrypted traffic detection database. If abnormal encrypted traffic is detected, the system records threat logs.

The system supports daily automatic update of the encrypted traffic detection database or you can manually update the database in real time. For more information, see the Updating Signature Database section of the "Upgrading System" on Page 1786 topic.

Configuring the Encrypted Traffic Detection Function

To configure the Encrypted Traffic Detection function, take the following steps:

1. Select **Object** > **Encrypted Traffic Detection**.



Option	Description
Detection Switch	Click the button to enable or disable the Encrypted Traffic Detection function. By default, this function is disabled.
Predefined Domain Whitelist	Click the button to enable or disable the predefined domain whitelist. By default, the whitelist is enabled. The predefined domain whitelist contains 10,000 common domain names. If traffic comes from a domain in the predefined domain whitelist, the traffic is considered as normal traffic and will not be detected by the Encrypted Traffic Detection function. You can update the

Option	Description
	predefined domain whitelist by updating the encrypted traffic detection database.
IP Whitelists	Traffic from the IP address or CIDR block in the whitelist is not detected by the Encrypted Traffic Detection function. To configure an IP whitelist, take the following steps: 1. Click **New**. The **Whitelist Configuration** panel appears. 2. In the Type field, specify the IP address type. Valid values: IPv4 and IPv6. 3. In the Content Type field, specify the content type of the IP whitelist. Valid values: Source IP based and Destination IP based. 4. In the Member field, add an address member to the IP whitelist. • If the Type parameter is set to IPv4, you need to specify the IPv4 address and subnet mask to be added to the whitelist. • If the Type parameter is set to IPv6, you need to specify the IPv6 address and prefix length to be added to the whitelist. Valid values of the prefix length: 120 to 128. 5. Click **OK**. You can view added IP whitelist entries in the IP whitelist list. To edit or delete an entry, select this entry and click **Edit** or **Delete**.

Option	Description
	Note: You can create up to 64 entries in the whitelist.

2. Click **OK**.



Notes: The Encrypted Traffic Detection function is supported for A-series (except A200/A1605/A1805/A2205/A6800/A7600) devices.

End Point Protection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

The endpoint security control center is used to monitor the security status of each access endpoint and the system information of the endpoint.

When the end point protection function is enabled, the device can obtain the endpoint data monitored by the endpoint security control center by interacting with it, and then specify the corresponding processing action according to the security status of endpoint, so as to control the endpoint network behavior.



Notes:

- At present, end point protection function only supports linkage with "JIANGMIN" endpoint security control center.
- End point protection is controlled by license. To use end point protection, apply and install the EPP license.

Related Topics:

- "Configuring End Point Protection" on Page 1453
- "Configuring End Point Security Control Center Parameters" on Page 1458
- "End Point Monitor" on Page 1526
- "EPP Log" on Page 1581

Configuring End Point Protection

This chapter includes the following sections:

- Preparation for configuring end point protection function.
- Configuring end point protection function.

Preparing

Before enabling end point protection, make the following preparations:

1. Make sure your system version supports end point protection.
2. Import an EPP license and reboot.

Configuring End Point Protection Function

The end point protection configurations are based on security zones or policies.

To realize the zone-based end point protection, take the following steps:

1. Create a zone. For more information, refer to "Security Zone" on Page 152.
2. In the **Zone Configuration**page, select **End Point Protection** tab.
3. Enable the end point protection you need and select an end point protection rule from the profile drop-down list below; or you can click **Add Profile** from the profile drop-down list. To create an endpoint protection rule, see Configuring End Point Protection Rule.
4. Click **OK** to save the settings.

To realize the policy-based endpoint protection, take the following steps:

1. Create a security policy rule. For more information, refer to "Security Policy" on Page 1089.
2. In the Policy Configuration page, expand Protection.

3. Select the **Enable** check box of **End Point Protection**. Then select an endpoint protection rule from the Profile drop-down list, or you can click **Add Profile** from the Profile drop-down list to create an end point protection rule. For more information, see Configuring End Point Protection Rule.

4. Click **OK** to save the settings.



Notes: When the zone and policy bind the same end point protection rule, the priority is policy > zone.

Configuring End Point Protection Rule

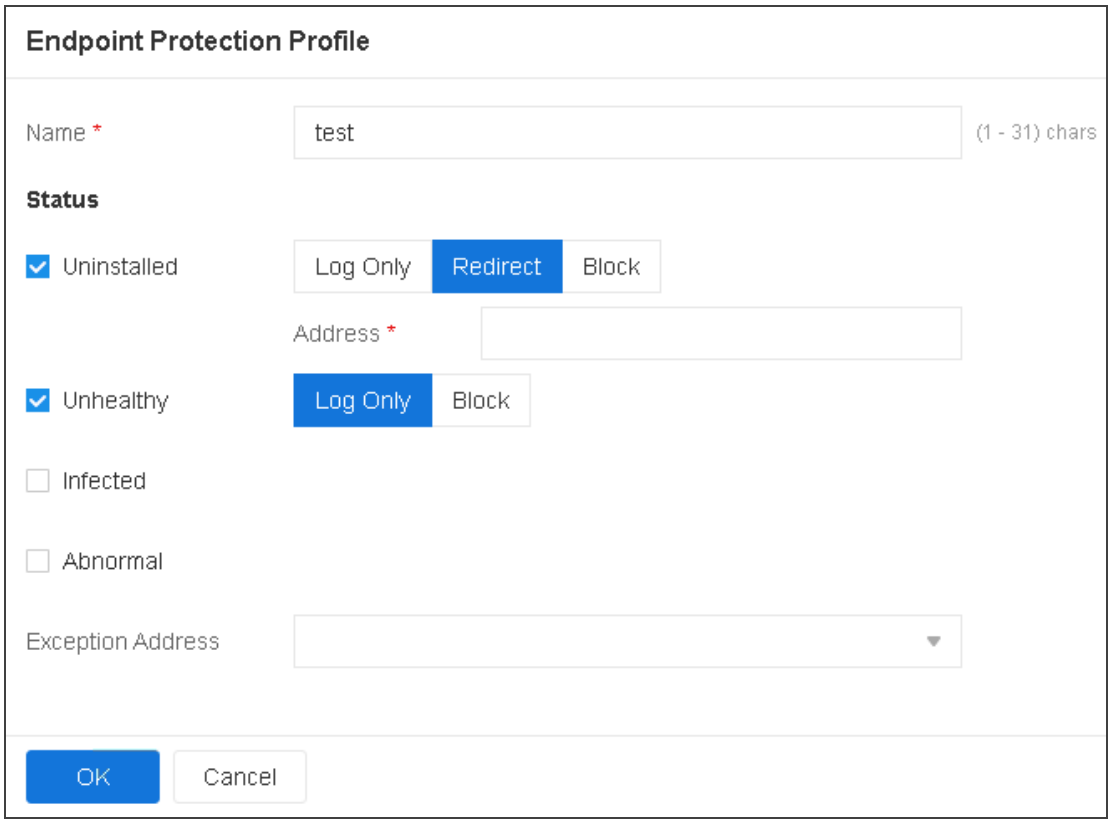
System has two default end point protection rules: **predef_epp** and **no_epp**.

- **predef_epp**: Execute the **Logonly** action for the endpoint whose status is "Uninstall" and "Unhealthy". Execute the **Block** action for the endpoint whose status is "Infected" and "Abnormal", and the block time is 60s.
- **no_epp**:No protective action is executed on all endpoints by default.

To configure an end point protection rule, take the following steps:

1. Click **Object> End Point Protection > Profile**.

2. Click **New**.



Option	Description
Name	Specifies the rule name.
Status	Specifies the protection action corresponding to the endpoint status. • Uninstalled: Specifies the protection action for the end-point which doesn't install an anti-virus client. Select the **Uninstalled** check box, and select the protection action in the drop-down list. • Redirect - Redirects the endpoint to the specified

Option	Description
	URL. Enter the URL in the **Address** text box. • Logonly - System will pass traffic and record logs only. • Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. The unit is second. The value ranges from 60 to 65535. • Unhealthy: Specifies the protection action for the unhealthy endpoint. Select the **Unhealthy** check box, and select the protection action in the drop-down list. • Logonly - System will pass traffic and record logs only. • Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. The unit is second. The value ranges from 60 to 65535. • Infected: Specifies the protection action for the infected endpoint. Select the **Infected** check box, and select the protection action in the drop-down list. • Logonly - System will pass traffic and record logs only. • Block - Block the endpoint connection, and spe-

Option	Description

	cifies the block time in the **Block time** text box. The unit is second. The value ranges from 60 to 65535.
	• Abnormal: Specifies the protection action for the abnormal endpoint. Select the **Abnormal** check box, and select the protection action in the drop-down list.
	  • Logonly - System will pass traffic and record logs only.
	  • Block - Block the endpoint connection, and specifies the block time in the **Block time** text box. The unit is second. The value ranges from 60 to 65535.

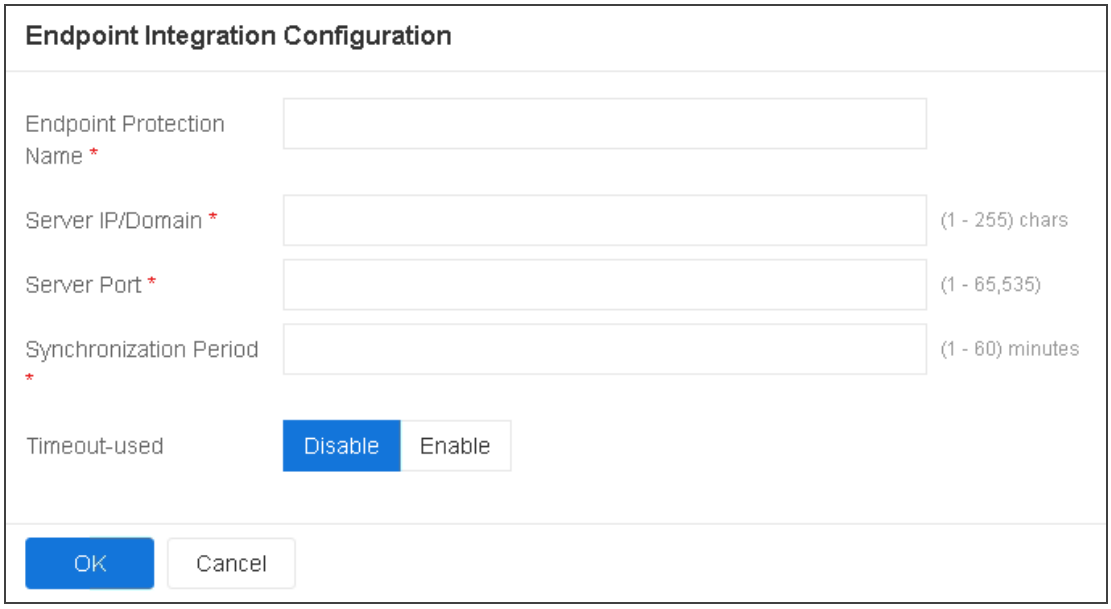
Exception Address	The exception address is not controlled by the end point protection rule. Select the address book name in the drop down list.  **Notes:** Before selecting the exception address, you need to add the exception endpoint address to the address book. For configuration, see "Address" on Page 814.

3. Click **OK** to save the settings.

Configuring End Point Security Control Center Parameters

To configure the endpoint security control center parameters, take the following steps:

1. Go to **System > Third Party Linkage**.
2. Click **New**.



Option	Description
Endpoint Prevention Name	Display the end point protection type as Jiangmin. Only one endpoint security control center server with the same type can be configured.
Server IP/Domain	Specifies the address or domain name of the endpoint security control center server. The range is 1 to 255 characters.
Server Port	Specifies the port of the endpoint security control center server. The range is 1 to 65535.
Synchronization Period	Specifies the synchronization period of endpoint data information. The range is 1 to 60 minutes. The default value is 10

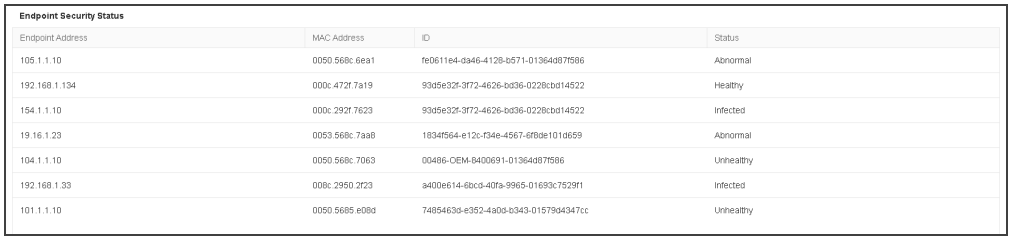
Option	Description
	minutes.
Timeout-used	• Disable: When the endpoint security control center is disconnected with the device and doesn't restore to connection in two synchronization periods, the synchronized endpoint data information will be cleared. By default, the timeout entry is disabled. • Enable: When the endpoint security control center is disconnected with the device and doesn't restore to connection in two synchronization periods, the endpoint data information that the system has been synchronized the last time continues to be used.

3. Click **OK**.

End Point Monitor

If system is configured with "Configuring End Point Security Control Center Parameters" on Page 1458, the endpoint detect page displays the endpoint data information list synchronized with the endpoint security control center.

Click **Monitor** > **End Point Monitor**.



IoT Monitor

The Internet of Things (IoT) refers to the billions of physical devices around the world that are now connected to the internet through information sensing devices, all collecting and sharing data for intelligent identification and management. The IoT technology is widely applied in large and medium-sized enterprises. Typically, in the IoT networks of these enterprises, there are various types of IoT devices, including video surveillance devices, access control systems, time attendance machines, facial recognition systems, office computers, televisions, IP phones, and more. However, with the increasing number of internal IoT devices within enterprises, it brings a series of security concerns such as devices being attacked by threats, controlled by botnets, and data leakage.

The system provides the overall IoT monitor function, which can implement the identification, security control, and threat management of IoT devices within the enterprise, and can protect devices from attacks and safeguard data privacy.

The IoT monitor function consists of the following four parts:

- **IoT Asset Identification**: The system supports two methods for identifying various types of IoT devices within the network: deploying the asset identification system in the Docker environment of the device, deploying the asset identification system in the virtual machine.
- **IoT Asset Management**: Monitor identified IoT devices in real time, combined with statistical analysis of the IoT devices. In addition, the system can manage assets in a unified manner.
- **IoT Policy Control**: Support to configure policy rules based on IoT devices. By analyzing the traffic flowing through the device, the system automatically maps the IP address to the IoT device object based on the attributes of the IoT device. This allows security policies automatically and dynamically manage and control the network permissions of the IoT device.
- **IoT Threat Management**: Combined with the threat protection function, endpoint protection function, and data security function in the system, IoT devices detected with security threats can be correspondingly governed.



Notes:

- The IoT montior function can identify IoT devices from the following manufacturers: Hikvision, Dahua, Uniview, Greenwill, Vivotek, Lenovo, Tiandy, Honeywell, Viewpointec, JSCT, Johnson Controls, Canon, HP, Epson, Samsung, Xiaomi, Huawei, JVC Kenwood, Netgear, Apple, Walkera, Foxconn, Schneider Electric, and Hillstone Networks.
- The IoT monitor function is controlled by license. In other words, this function is available only after the IoT license is installed for devices that support the IoT monitor function.
- The IoT monitor function cannot be used to identify IoT devices in a NAT scenario.
- In deployment environments that use the IoT monitor function, DHCP traffic from IoT devices needs to pass through the firewall or mirror the traffic to the firewall.

Typical Deployment Scenario

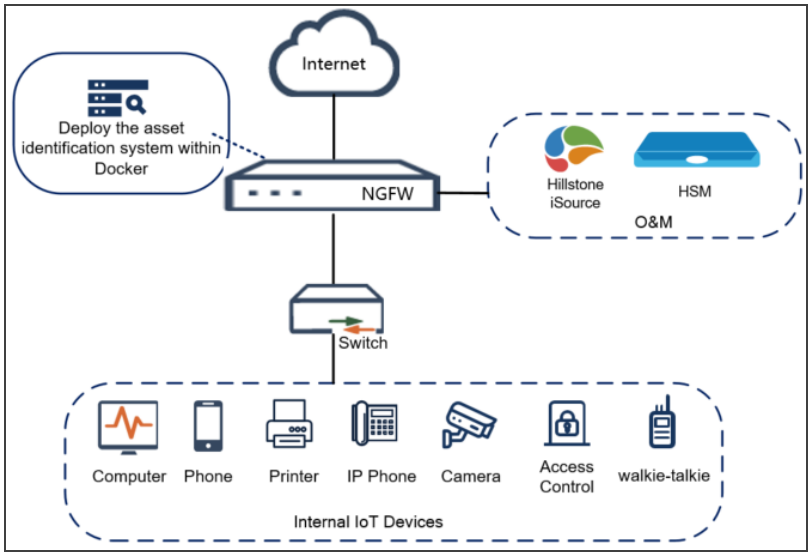
The typical deployment method of IoT monitor includes:

- **Local Asset Identification**: Identify information about IoT device assets based on the local asset identification module, which is divided into the following two types:
  - Built-in: Use the Docker management function of the system to deploy the asset identification system within the firewall.
  - External: Install the asset identification program on the virtual machine and use the asset identification system deployed on the virtual machine.

Notes: The built-in type for local asset identification is available only for A-series firewalls. We recommend that you use A2600 and later (A2600- A3815 need to be installed with an SSD, and A5100 and higher models can be installed with an SSD).

Built-in Asset Identification

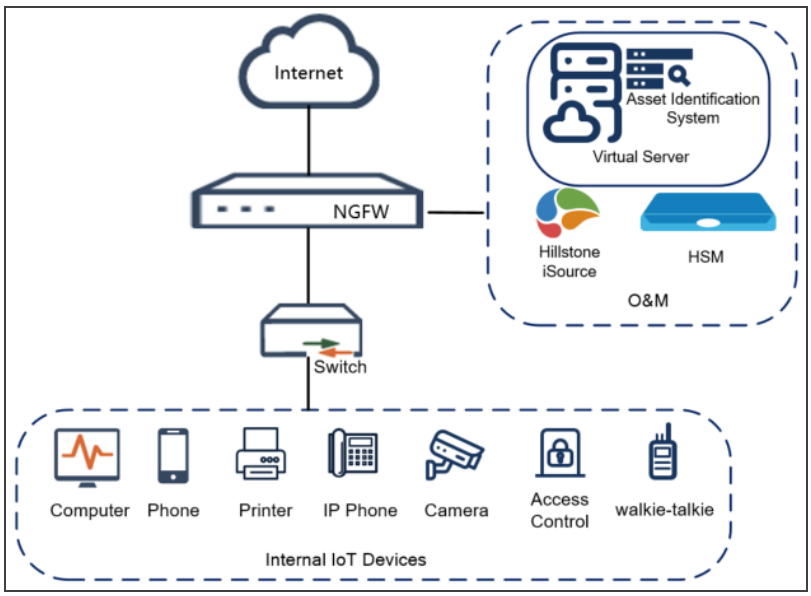
As shown in the figure below, the internal IoT of the enterprise contains various types of IoT devices, such as video surveillance devices, access control systems, office computers, IP phones, mobile phones, and walkie-talkies. A firewall (NGFW) is deployed in the enterprise, and the asset identification system is deployed into the system by using the Docker management function of the firewall to identify IoT device asset information, which is used in conjunction with the IoT monitor function of the firewall to implement security control. Meanwhile, HSM and iSource are deployed to upload IoT asset data for further security control and threat governance.



External Asset Identification

As shown in the figure below, the internal IoT of the enterprise contains various types of IoT devices, such as video surveillance devices, access control systems, office computers, IP phones, mobile phones, and walkie-talkies. A firewall (NGFW) is deployed in the enterprise, and the asset identification system is installed and deployed on the virtual server to identify IoT device asset

information, which is used in conjunction with the IoT monitor function of the firewall to implement security control. Meanwhile, HSM and iSource are deployed to upload IoT asset data for further security control and threat governance.



Configuration Procedure of IoT Monitor Function

To use the IoT monitor function, you need to configure the following:

1. IoT Asset Identification

    a. Select an IoT asset identification type:

    - Local asset identification: built-in——use the Docker management function to deploy the asset identification system into the device system; external——install the asset identification program on the virtual machine and use the asset identification system deployed on the virtual machine.

    b. Configuring IoT global configuration——Specify the asset identification method and the corresponding detailed configuration.

    c. Configuring the identification list——Specify the address list of IoT asset devices that you want to identify.

d. Configuring the endpoint type——Enable/disable the function of automatically synchronizing endpoints to the repository.

e. Configuring the zone——Enable the IoT Monitor function within a zone and bind the identification list. Note: To resolve HTTP traffic, enable the Intrusion Prevention function at the same time.

2. IoT Monitor Management

a. Configuring the region——Add the region of the corresponding area for IoT devices.

b. Viewing IoT monitor——View the manufacturer, type, online devices, and various detailed statistics of all identified IoT devices.

c. Viewing IoT logs

3. IoT Policy Control

a. Configuring the device object——Specify classification dimensions for IoT devices, such as manufacturer, type, device model, operating system, etc. The system will then map the identified IoT device information to corresponding device objects.

b. Configuring the policy rule——Configure the policy rule based on device objects.

4. IoT Threat Governance

a. Combined with the threat protection function, endpoint protection function, and data security function, IoT devices detected with security threats can be correspondingly governed.

b. Uploading IoT data to iSource——You can implement further threat event response and handling such as asset management and policy/blocking deployment by using iSoutce.

c. Uploading IoT data to the Hillstone cloud platform——Upload IoT report data and asset data to the cloud platform for unified analysis, statistics, and management.

Notes: The IoT monitor function is controlled by license. Make sure that the current device supports the IoT monitor function and is installed with the IoT license.

Deploying the Asset Identification System on the Virtual Machine

When you use the external local asset identification type, you can deploy the asset identification system on the virtual machine.

This topic describes how to deploy the asset identification system in different environments, including VMware and OpenStack. Before the deployment, you need to be familar with VMware and OpenStack.

- Deploying the asset identification system on VMware ESXi
- Deploying the asset identification system on OpenStack

Deploying the Asset Identification System on VMware ESXi

You can deploy the asset identification system on an X86 device that supports the VMware ESXi virtual machine by importing the OVF+VMDK file. After the deployment is completed, you can automatically update the identification engine version by using Update Server.

Before You Start

Before you deploy the asset identification system on the VMware ESXi server, make sure:

- You are familiar with the vSphere Hypervisor structure, ESXi host settings, and virtual machine deployment of VMware.
- Prepare the virtual machine environment based on the system requirements and limits and set up the ESXi Server host.
- Contact the customer service personnel of Hillstone to obtain the installation file (in the ZIP format) that contains ovf, vmdk, iso and mf files, unzip it, and save the ovf and vmdk files to your PC.

System Requirements and Limits

To deploy the asset identification system on VMware ESXi, the VMware ESXi server needs to be:

- VMware ESXi 7.0 or later.
- Requires at least 4 vCPU, 4GB memory, 20 GB disk space, and NIC is installed.

Procedure

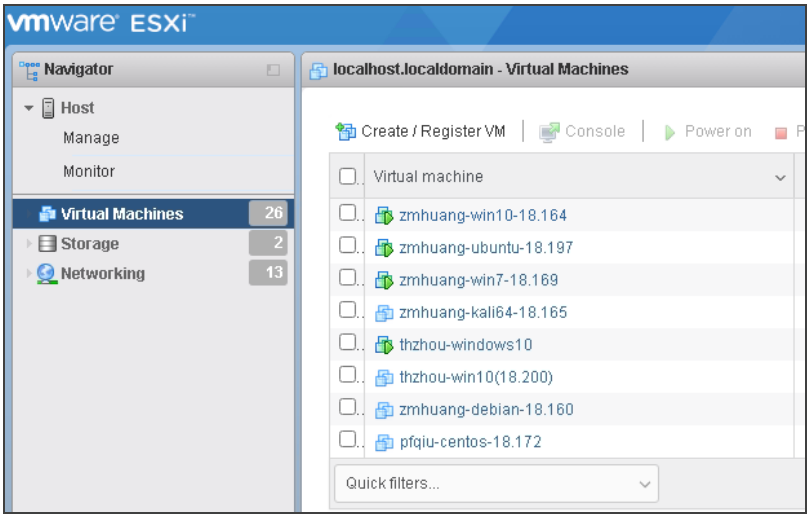
In the following example, VMware ESXi 7.0 is used.

Step 1: Log in to VMware ESXi

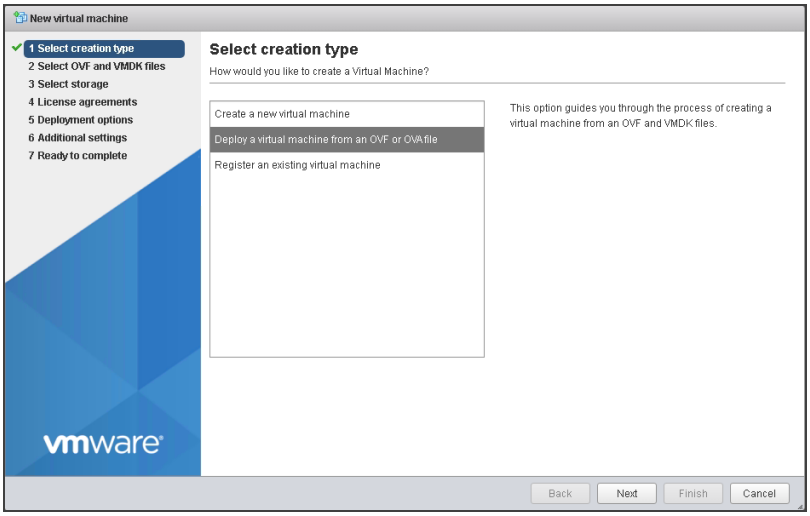
To access VMware ESXi 7.0, enter the username and password and click Login.

Step 2: Create a VM

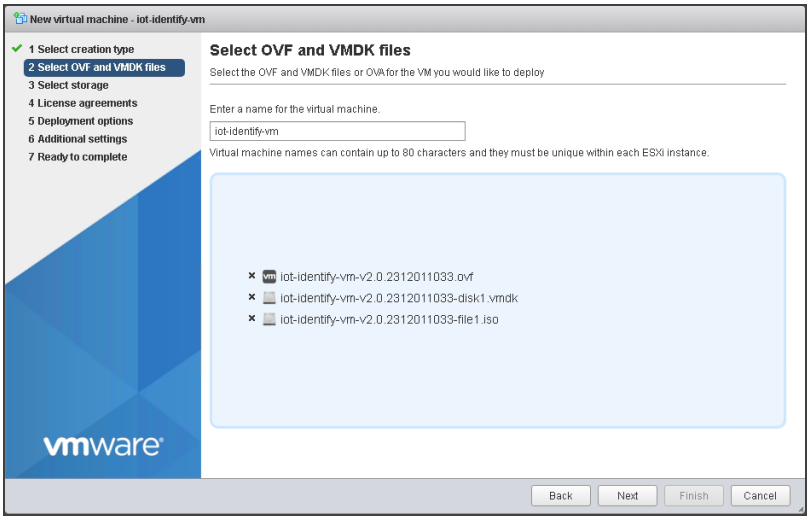
1. After you log in to VMware ESXi 7.0, click **Virtual Machines** in the left-side navigation pane. On the page that appears, click **Create/Register VM**.



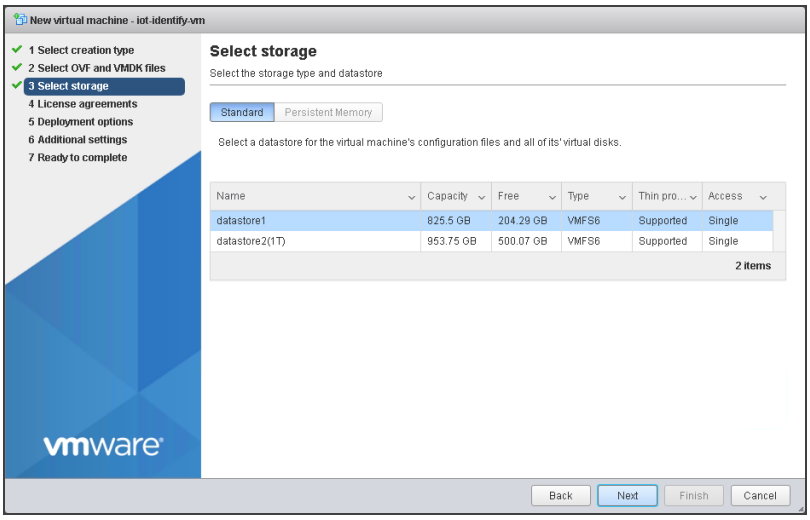
2. In the **New virtual machine** dialog box, select **1 Select creation type** > **Deploy a virtual machine from an OVF file**, and click **Next**.



3. Enter a name for the VM, and click the upload section to select the OVF and VMDK files or drag the file to the upload section. Then, click **Next**.

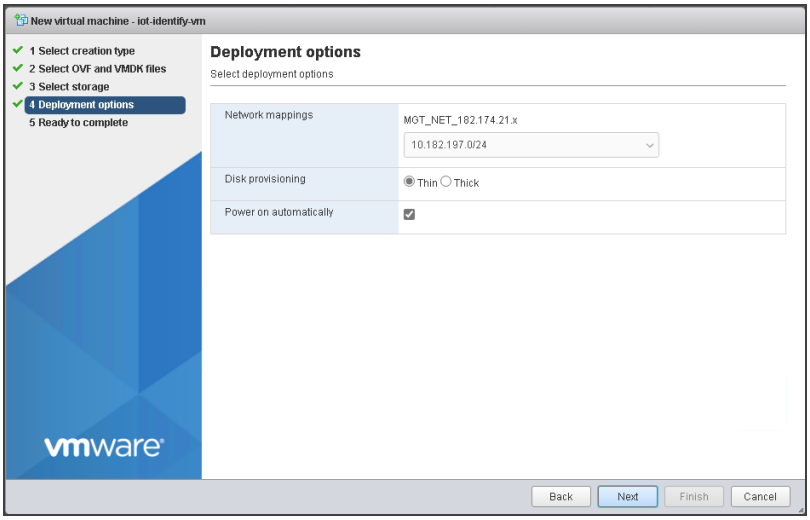


4. Select a storage type and datastore and click **Next**.



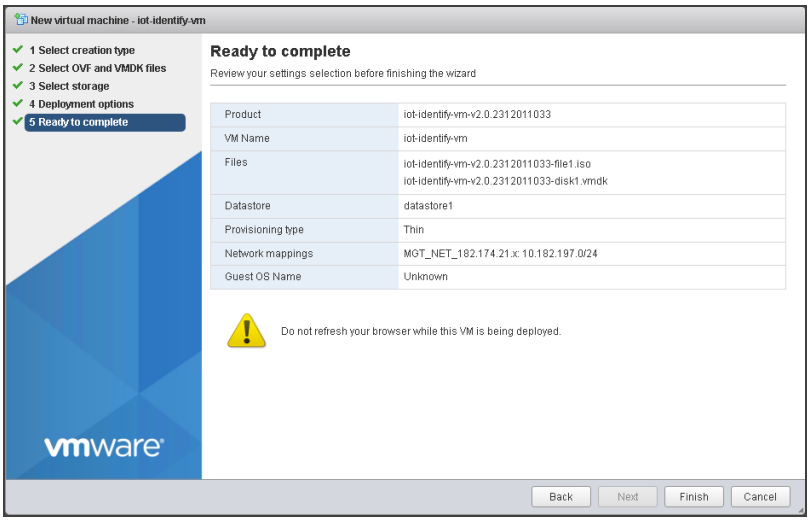
Note: The hard disk needs to be at least 20 GB in size.

5. Select deployment options. Set the **Network mappings** parameter based on your network environment and set the **Disk provisioning** parameter to **Thin**. Then, click **Next**.



Note: "Thick device" consumes more disk space.

6. After you check that the configurations are correct, click **Finish**. You can ignore error messages.



7. After the system files are uploaded to the disk, the VM is created.

Notes: The procedure may take a long time. Please do not refresh the page and wait until the deployment is completed.

Step 3: Log in to the virtual machine

1. After the virtual machine is created, it is automatically powered on and started.
2. In the left-side Navigator, click Virtual Machine and then select the virtual machine created in Step 2.
3. Select **Console** > **Open browser console** or click the console thumbnail to open the console.
4. Enter the default username and password (hillstone/hillstone) to lo in to the virtual machine.

Step 4: Configure NIC

After the virtual machine is deployed, you need to configure the configuration file within /etc/netplan to modify the NIC configuration based on the current environment.

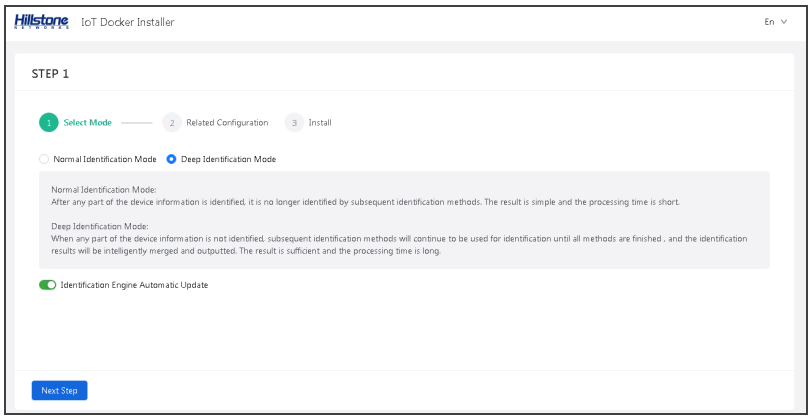
1. In the console, run the **cat /etc/netplan/00-installer-config.yaml** command to view the current configuration file.
2. Run the **vi /etc/netplan/00-installer-config.yaml** to open the configuration file.
3. Move the cursor to the position where you want to modify and press **i** to enter the editing mode. You can modify the IP address, gateway address, or configure DHCP.
   Note: The IP address needs to be accessible by the firewall and the browser of the PC on which the asset identification system is installed. This IP address is used as that of the IoT local asset identification virtual machine. (In this example, 10.182.197.172 is used)
4. Press "ESC" and then **:wq** to exit the configuration file and save the configuration.
5. Restart the virtual machine to ensure the modified NIC information.

Step 5: Install the asset identification program

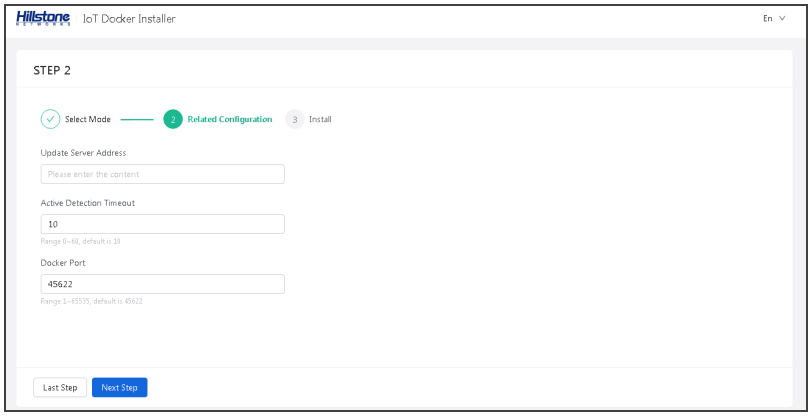
1. Open the browser and access the IP address configured in Step 4. Example: https://10.182.197.172:22654

2. Due to the use of a self-signed certificate, the browser displays a warning: 'Your connection is not private'. Click **Advanced** > **Proceed** to continue accessing the site.

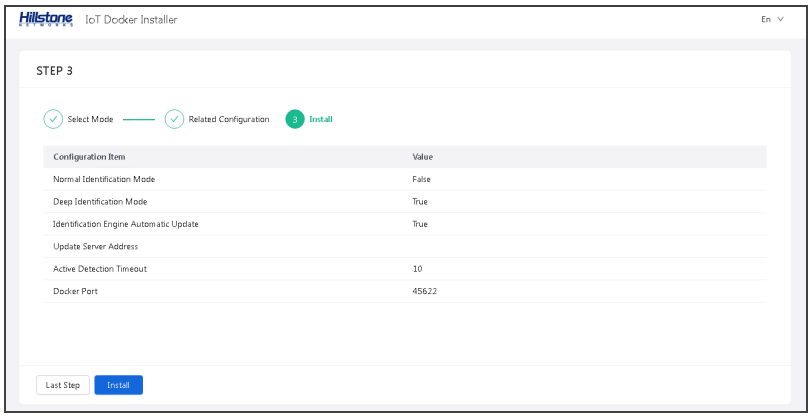
3. Enter the asset identification program installation guide. Select an identification mode and click **Next**. By default, **Deep Identification Mode** is selected and **Identification Engine Automatic Update** is enabled.



4. In the **Related Configuration** step, configure the Update Server address, active detection timeout, and Docker port number. If you use the default configuration, Update Server provided by Hillstone Networks is used.



5. Confirm the configuration and click **Install**.



6. After the installation is completed, the asset identification program is automatically started.

At this point, the asset identification system is deployed on VMware ESXi.

Deploying the Asset Identification System on Openstack

Before You Start

Before you deploy the asset identification system on Openstack, make sure:

- Prepare the host environment based on the system requirements.
- Contact the customer service personnel of Hillstone to obtain the image file of the asset identification system in qcow2 format and store the file to your PC.

System Requirements

To deploy the asset identification system on an OpenStack platform, the following requirements need to be met:

- Requires at least 4 CPU and 4 GB memory.

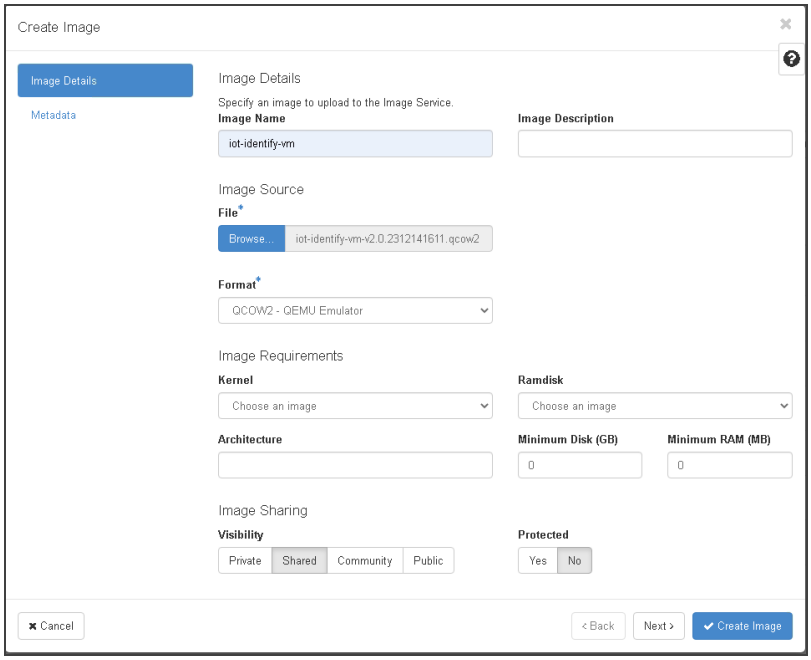
- Openstack and its components Horizon, Nova, Neutron, Glance, and Cinder are installed. (For more information about how to install Openstack, see http://-docs.Openstack.org/icehouse/install-guide/install/apt/content/)

Procedure

Step 1: Import the Image File

1. Log in to the OpenStack WebUI with a normal account, and select **Project** > **Compute**> **Images**.

2. Click **Create Image** on the top right corner.



3. In the <Create Image> dialog, configure following options.

Option	Description
Image Name	Enter the name of the image, such as "iot-identity-vm".
File	Click **Browse**, and select the image file in the qcow2 format from the local PC.

Option	Description
Format	Select **QCOW2-QEMUEmulator** from the **Format** drop-down list.

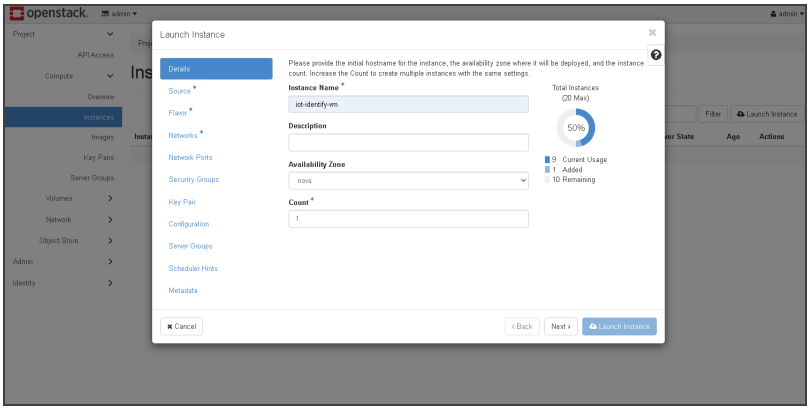
4. Keep other information as default.
5. Click **Create Image**.
6. Wait a few moments, it takes about 10 minutes. The image file will be imported successfully and displayed in the list.

Step 2: Create a Flavor

Normally, a non-admin user cannot change the properties of an instance, including core, and memory. If you want to change an instance, you can change the flavor it belongs to, since the instance inherits what its flavor has.

To create a flavor, take the following steps:

1. Log in to OpenStack WebUI with the admin account.
2. Select **Admin**> **System**> **Flavors**, and click **Create Flavor** on the top right corner.



3. In the <Create Flavor> dialog, configure the flavor.

Option	Description
Name	Enter the flavor name, such as "iot.normal".
ID	Skip this step since ID is automatically generated by OpenStack.
VCPUs	Specify the number of CPU cores. "4" is recommended and "2" is the lowest configuration.
RAM (MB)	Specify the RAM size of the virtual machine. "4096MB" is recommended and "2048MB" is the lowest configuration.
Root Disk (GB)	Specify the size of root disk .The minimum is 8 GB. We recommend that you set the size to 20 GB.

4. Click **Create Flavor** in the lower-right corner.

Step 3: Create a Network

The network services of OpenStack provide scalable network connectivity for OpenStack cloud deployments. On the OpenStack WebUI, you can create and modify networks.

This document does not describe how to create a network because different users have different networking needs and creating a network is a basic operation of Openstack. For more information, see http://docs.Openstack.org/user-guide/content/dashboard_create_networks.html

In most cases, there is usually an external network, such as 'ext-net,' available in the OpenStack environment, which you can use directly.

Step 4: Start the Instance

Log in to OpenStack WebUI with admin account. To create an instance, take the following steps:

1. Select **Project** > **Compute** > **Instance** , and click **Launch** after the image list created in Step 1.



2. In the < Launch Instance> dialog box, configure the followings.
3. In the <Details> tab, enter the **Instance Name**, such as "iot-identify-vm".
4. In the <Source> tab, you can select **No** for **Create New Volume**.
5. In the <Flavor>tab, select the flavor "iot.normal" configured in step 2.
6. In <Networks> tab, select the network "ext-net" and click  so that the instance can be accessible externally.
7. Keep the other information as default.
8. Click **Create Instance** in the lower-right corner. In most cases, the instance will be automatically started after created.
9. After the instance is created, an IP address is assigned to the instance. You can use this IP address as that of the virtual machine of IoT local asset identification.

Step 5: Log in to Virtual Machine

1. Log in to OpenStack WebUI.
2. Select **Project** > **Compute**> **Instance**.
3. In the list, click the instance name "iot-identify-vm" to go to the instance details page. You can click the Console tab to open the console page in the embedded CLI.
4. Enter the default username and password (hillstone/hillstone) to log in to the virtual machine.

Setp 6: Configure NIC

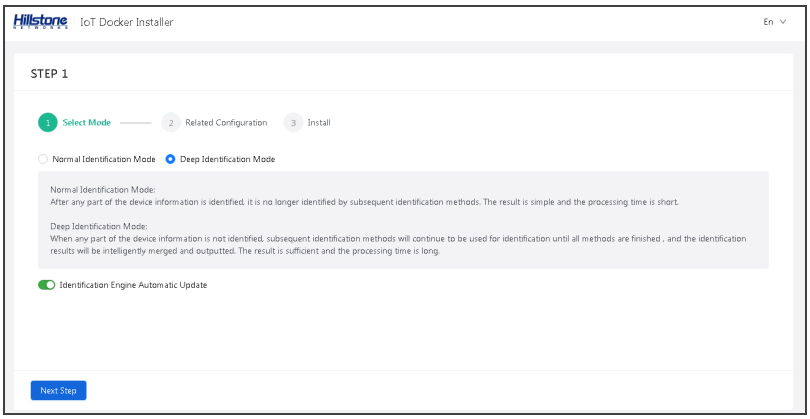
After the virtual machine is deployed, you need to configure the configuration file within /etc/netplan to modify the NIC configuration based on the current environment.

1. Confirm the NIC name. Run the **ip addr** command to view the current NIC name. The default NIC name is "ens160". The default NIC name that is automatically assigned may vary based on deployment environments.
2. Run the **cat /etc/netplan/00-installer-config.yaml** command to view the current configuration file.
3. Run the **vi /etc/netplan/00-installer-config.yaml** command to open the configuration file.
4. Move the cursor to the position where you want to modify and enter **i** to enter the editing mode. You can modify the NIC name and NIC number.
   Note: The NIC name needs to be consistent with the confirmed NIC name.
5. Press "ESC" and then enter **:wq** to exit the configuration file and save the configuration.
6. Restart the virtual machine to ensure the modified NIC information.

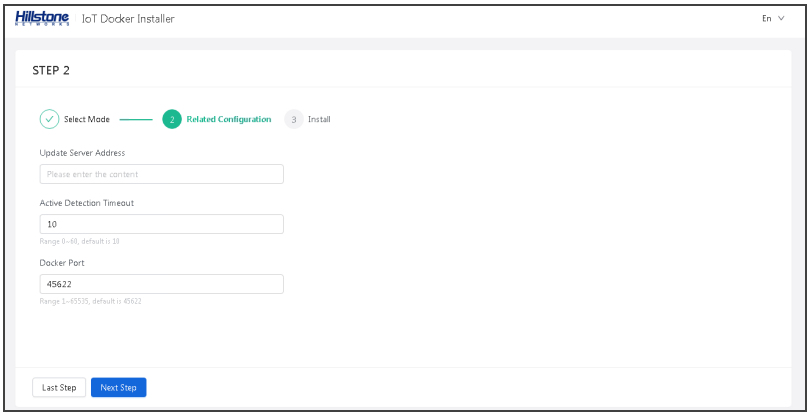
Step 7: Install the asset identification program

1. Open the browser and access the IP address configured in NIC information. Example: https://10.182.237.89:22654
2. Due to the use of a self-signed certificate, the browser displays a warning: 'Your connection is not private'. Click **Advanced** > **Proceed** to continue accessing the site.
3. Enter the asset identification program installation guide. Select an identification mode and click **Next**. By default, **Deep Identification Mode** is selected and **Identification Engine**

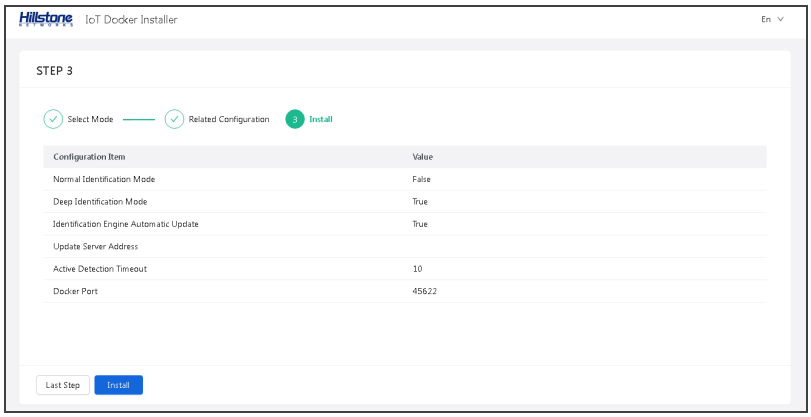
Automatic Update is enabled.



4. In the **Related Configuration** step, configure the Update Server address, active detection timeout, and Docker port number. If you use the default configuration, Update Server provided by Hillstone Networks is used.



5. Confirm the configuration and click **Install**.



6. After the installation is completed, the asset identification program is automatically started.

At this point, the asset identification system is deployed on OpenStack.

Identification List

For the traffic flowing through the zone bound with the identification list, the system supports to identify IoT devices by configuring the identification list of the IP, MAC and IP/MAC types.

When the identification lists of the IP/MAC, IP and MAC types are all configured, traffic matches the identification lists in the sequence of IP/MAC > IP > MAC.

Notes: The maximum number of identification lists that can be configured/imported varies based on platforms. In addition, the number of IP/MAC, IP, and MAC addresses that can be added to the identification list varies. For example, if the current device allows up to 1,500 identification lists to be configured/imported, the ratio of the maximum number of IP/MAC, IP, and MAC addresses allowed to be added to the identification list is 2:1:2. In other words, the maximum number of IP/MAC addresses is 600, the maximum number of IP addresses is 300, and the maximum number of MAC addresses is 600.

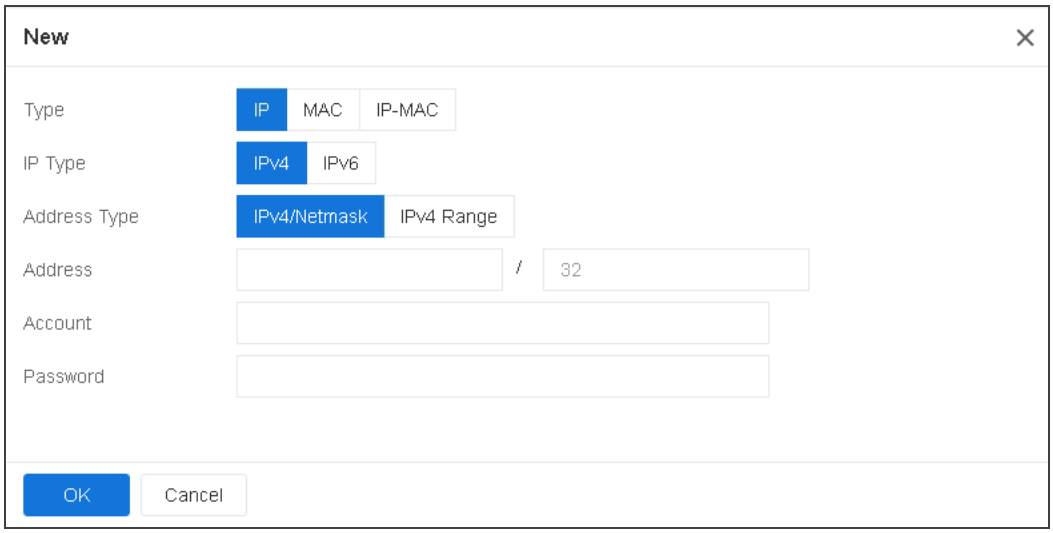
Configuring the Identification List

You can configure the identification list by using one of the following methods:

- Creating Identification List Profile
- Importing Identification List

Creating Identification List Profile

1. Select **Object** > **IoT Policy** > **Identification List**.
2. Click **New**. In the **Name** field, enter the name of the identification list. Then, click **New**.



Option	Description
Type	Specifies the type of the identification list. Valid values: **IP**, **MAC**, and **IP-MAC**. Note: When the IoT device is not in the same broadcast domain as the Hillstone device, the IoT device cannot match the identification list because the MAC address obtained in the packet may not be the real address. In this case, we recommend that you set the type to **IP**.
IP	If you set the type to IP, you need to select the IP type of IoT device.

Option	Description

	• IP Type: Select the IP type of IoT device. IPv6 is available only when the current version supports IPv6.
	  • IPv4/Netmask: Enter the IPv4 address and subnet mask.
	  • IPv4 Range: Enter the start IPv4 address and end IPv4 address.
	  • IPv6/Prefix: Enter the IPv6 address and prefix length.
	  • IPv6 Range: Enter the start IPv6 address and end IPv6 address.
	• Account (optional): Enter the username that manages the IoT device.
	• Password (Optional): Enter the password corresponding to the username.

MAC	If you set the type to MAC, you need to enter the MAC address of IoT device.
IP-MAC	If you set the type to IP-MAC, you need to select the IP type of IoT device. • IP Type: Select the IP type of IoT device. IPv6 is available only when the current version supports IPv6. • IPv4: Enter the IPv4 address.

Option	Description
	• IPv6: Enter the IPv6 address. • MAC: Enter the MAC address. • Account (optional): Enter the username that manages the IoT device. • Password (Optional): Enter the password corresponding to the username.

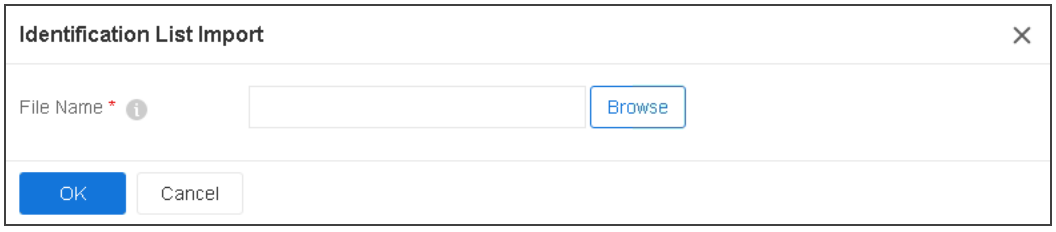
3. Click **OK**.

Notes: The identification list of the specified type in one profile cannot be repeated, otherwise, an error will pop up. The repeat conditions for different types include:

- IP-MAC: The IP address and MAC address are the same.
- IP: There're repeated IP addresses in the IP/netmask or IP range.
- MAC: The MAC addresses are repeated.

Importing Identification List

1. Select **Object** > **IoT Policy** > **Identification List**.
2. (Optional) Click **Identification List Template** and download the template in local.
3. Select an identification list and click **Import**.



4. In the **Identification List Import** dialog, click **Browse** and upload the identification list in the local.

5. Click **OK**.

Configuring Region

Click **Object** > **IoT Policy**. The **Region Setting** page displays the region by region level. On this page, you can configure regions and deploy network video monitor devices to the corresponding region based on IP address. After you click a region node in the left-side pane, the right-side section displays address members and hierarchical relationships of all sub-regions within this region; if there is no sub-regions within this region, then display the address members and hierarchical relationships of this region.

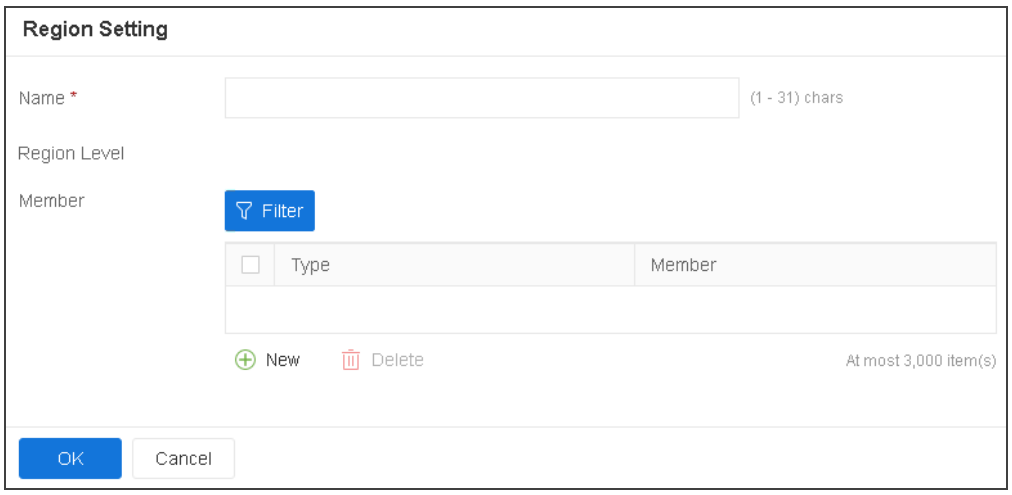
The deployment information will be displayed in the **Deployment Area** column on the **Monitor** > **IoT Monitor** > **Details**.

Creating a Region

To create a region and add IoT devices to the corresponding region according to the IP address, take the following steps:

1. Select **Object** > **IoT Policy** > **Region Setting**.

2. Click **New**.



Note: To create a next-level region under an existing region, you need to select the existing

region and click **New**.

On the Region Setting page, configure the following options:

Option	Description
Name	Enter the region name, which can be 1 to 31 characters.
Region Level	Displays the parent region of the current region.
Member	Click **New** to configure an address member in the region. • Type: If the IP type is IPv4(IPv6), select IP/Netmask (IPv6/Prefix) or IP Range(IPv6 Range) from the **Type** drop-down list. • Member: Enter the corresponding address information. **Note:** At most 4 levels of areas can be configured. The IPv6 address is valid only when the system version is the IPv6 version.
	To delete an address member, select it and click **Delete**.

3. Click **OK**.

Terminal Type

Click **Object** > **IoT Policy**. The **Terminal Type** page displays device types supported by IoT Policy. You can add device types to or remove device types from the repository as required.



- You can turn on the switch in the **Add to Repository Automatically** column to automatically add the terminal to the repository. By default, this function is disabled for all device types.

Checking Whether Device is in Repository

To check whether a device is in the repository, take the following steps:

1. Select **Monitor** > **IoT Monitor** > **Details**.
2. Check whether the device in the repository in the **In Repository or Not** column.

Filtering Repository Devices

To filter repository devices, take the following steps:

1. Select **Monitor** > **IoT Monitor** > **Details**.
2. Click Filter, add the **In Repository or Not** filter condition, and then select **yes**.
3. This way, you can view all devices that are in the repository.

Configuring IoT Global Configuration

IoT global configuration includes:

- Uploading IoT data to the cloud platform of Hillstone
- Configuring local asset identification

Select **Object** > **IoT Policy** > **Configuration**.

Option	Description
Upload IoT Data	Connect to the cloud platform and upload IoT report data and asset data to this platform for unified analysis and statistics. This option displays whether **Upload IoT Data** is enabled. You can click **Configure**. In the **Connecting to Hillstone Cloud Service Platform** panel, select the IoT report data or asset data in the Upload Data Item section.
Local Asset Identification	Identify IoT device assets by using the local asset identification module. To enable this function, turn on the switch.
Asset Identification Module Type	Local asset identification is divided into built-in and external types. • Local: Use the built-in asset identification module. Before you select this type, configure the Docker management function of the system to deploy the asset identification system within the firewall. • External: Use the asset identification system deployed on the virtual machine. Before you select this type, deploy the asset identification system in the virtual machine. **Note**: The "Local" type for local asset identification is available only for A-series firewalls. We recommend that you use A2600 and later.
IP	When you select "Local", this IP address is the default IP address of the built-in asset identification module: 127.0.0.1. When you select "External", enter the IP address of the virtual

Option	Description
	machine.
Port	Specifies the port number of the asset identification module. When you select "Local", this port number is the host port number of Docker. Please make sure this port number is consistent with the host port number specified in Docker. Valid values: 1-65535.
Virtual Router	If you select "External", select a VRouter to which the virtual machine belongs from the drop-down list.

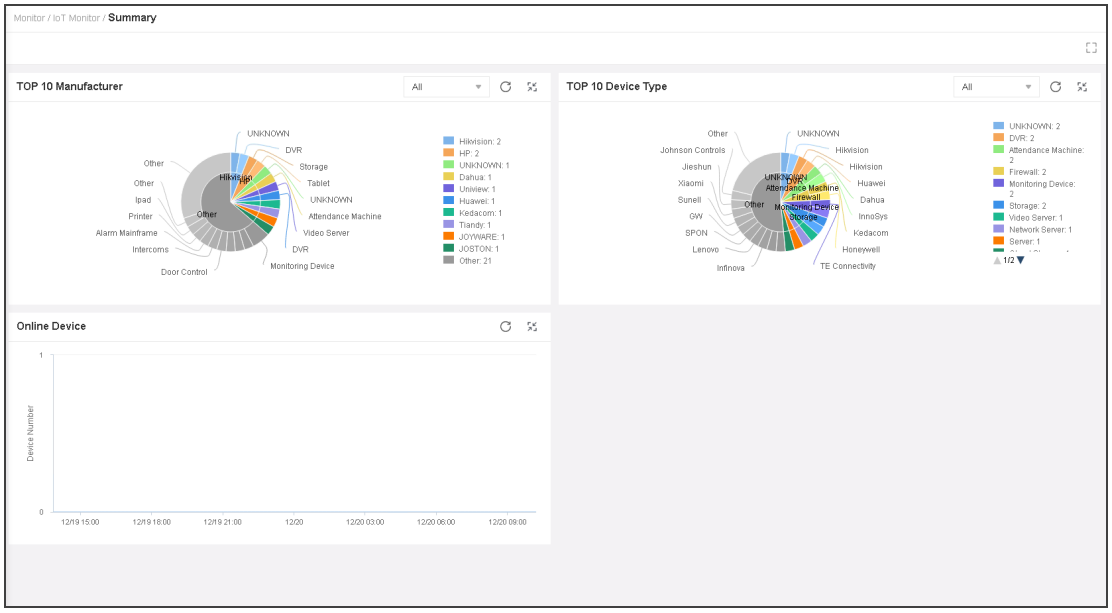
IoT Monitor

IoT Monitor function displays the manufacturers and types distribution of network video monitoring devices, as well as the detailed statistics, such as device number, IP address, MAC address, up/downstream traffic, IoT profile and device status.

Summary

On the Summary page, you can obtain the real-time distribution of manufacturers and device types.

Click **Monitor** > **IoT Monitor** > **Summary**.

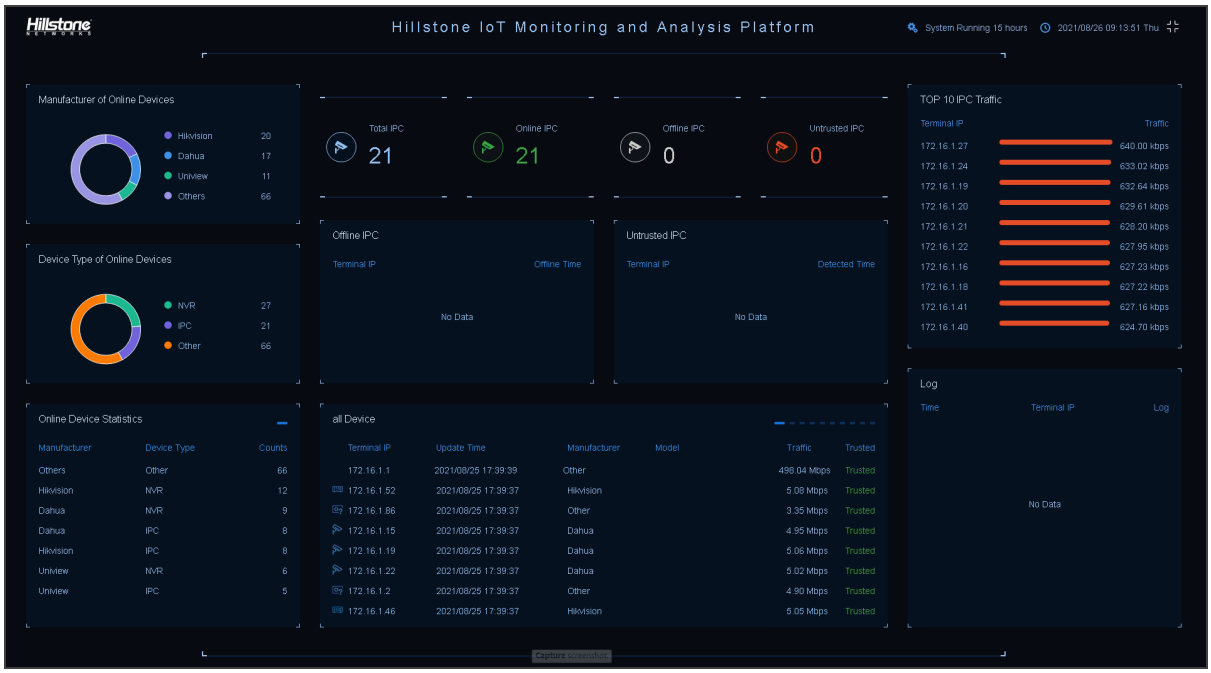


- Select Online/Offline/All from the drop-down list in the upper-right corner to view manufacturers and device types in the corresponding status.
- Click the button to refresh the monitoring data.
- Hover your mouse over the bar chart to view the device number of different manufacturers and different device types.
- Hover your mouse over the line chart to view the number of online devices.
- Different manufactures and devices are marked with different colors of legends. When your mouse hovers over an legend, the corresponded part will be highlighted on the bar chart.
- Click the button to enter the screening monitoring mode.

Screening Monitoring Mode

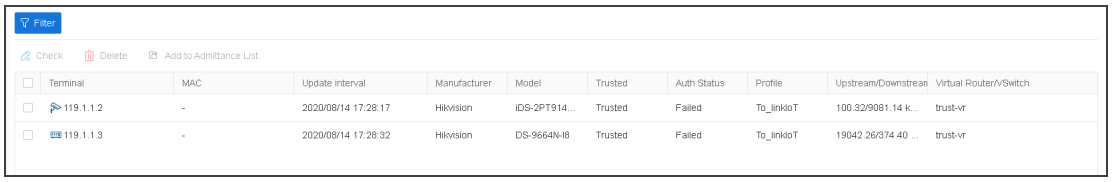
The screening monitoring mode of IoT monitor displays various statistical information such as the manufacturer, type, number of cameras, and traffic of online network video monitoring device in a more intuitive way.

Click the button in the upper right corner of the summary page to enter the screening monitoring mode.



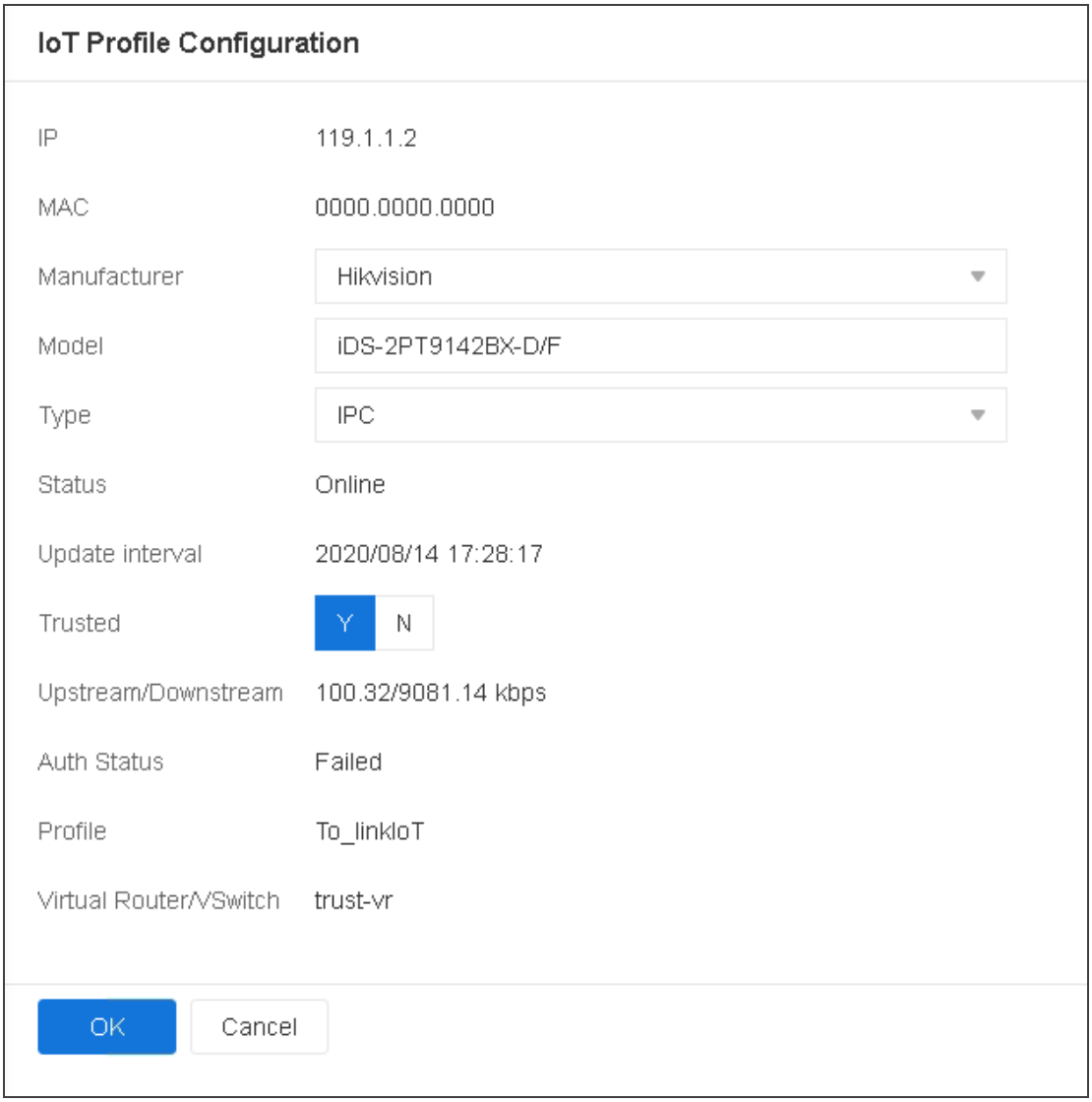
Details

Click **Monitor** > **IoT Monitor** > **Details** to view the detailed information of the network video monitoring devices.



- Click the Filter button to add filter conditions and the required information will be filtered out in the following list.
- Select the check box, and click **Delete** to delete the selected item.
- Select the check box, and click **Check**, then the **IoT Profile Configuration** page pops up. You can modify the manufacturer, model, type and trust status manually. The manually changed

configuration is prior to the automatically detected result. When the device logs in again, the manually changed configurations will be cleared.



- Select the check box and click **Add to Admittance List** to add the selected item to the target admittance list template. For the detailed steps, refer to Adding to Admittance List.
- Click **Add to Respository** to add the selected network video monitor device to the repository.

- Click **Remove From Respository** to remove the selected network video monitor device from the repository.
- For the icons in the **Terminal** list, if the icon is gray, it means that the device is offline; if the icon is blue, it means that the device is online. When you hover the mouse over the icon, you can also view the online status of the device. The icons represent the following devices respectively:
  - : The network video monitoring devices of other manufacturers.
  - : The IPC device.
  - : The NVR device.
  - Null: The item hasn't been identified.

IoT Log

You can view, configure, clear or export IoT logs.

The following condition should be met before log's generation:

- The IoT logging function has been enabled on the device. For the detailed configurations, refer to Log Management.

Click **Monitor** > **Log** > **IoT Log** to enter the <IoT Log> page.

- Click the 

button to add filter conditions and the required information will be filtered out in the following list.
- Configure: Click the **Configure** button and enter the **Log Management** page.
- Clear: Click the **Clear** button to delete all the filtered IoT logs in system.

- Export: Click the **Export** button to export part or all logs in the format of TXT or CSV. Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.

Cloud-Network Collaborative DNS Protection

The Domain Name System (DNS) is a critical component of network communication, and its security is vital for maintaining the overall safety of the network environment. Attackers often exploit DNS's widespread presence and high traffic to mask malicious activities. Research shows that up to 80% of malware uses DNS to initiate command-and-control programs. Consequently, implementing effective DNS security detection not only uncovers potential network threats but is also crucial in preventing malware propagation and data breaches.

Hillstone Networks offers several cloud-network collaborative DNS security solutions:

- Unknown Domain Cloud Collaborative Query: Collaborating with CloudVista, the system continuously enhances threat detection capabilities by leveraging vast cloud-based threat intelligence. It performs real-time cloud queries to assess the risk status of unknown domains. Coupled with the botnet prevention function, this solution effectively intercepts risky DNS traffic at the internet egress.
- Cloud-Based DNS Security Detection: Integrating with secure DNS SaaS services, this solution proxies and forwards DNS traffic from the internal network to the cloud for domain resolution via DoH (DNS over HTTPS). This ensures the integrity and confidentiality of the resolution process. In addition, the cloud can identify and block malicious domains using extensive threat intelligence, effectively safeguarding internal network hosts.

Unknown Domain Cloud Collaborative Query

Introduction

For domains that are not included in the botnet address library, exception list, or block list (referred to as "unknown domains" in this context), there may be challenges in controlling and defending against them by using the botnet prevention function.

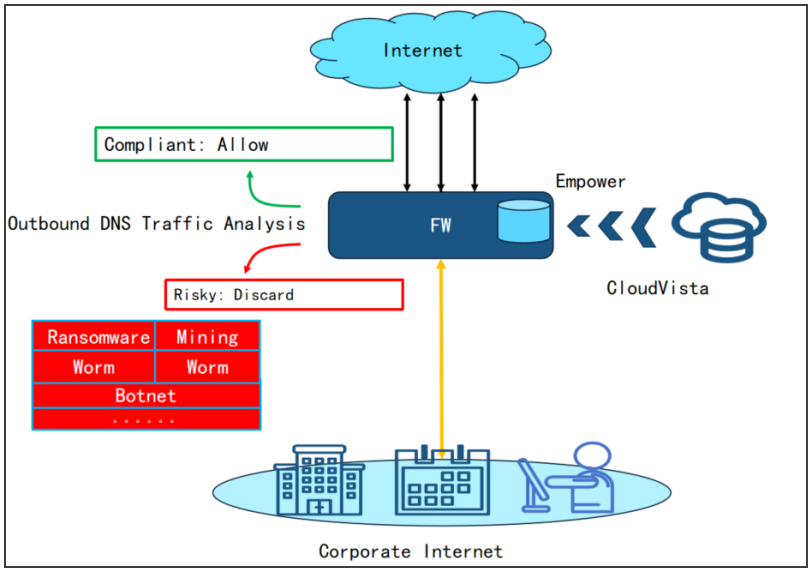
The system provides the Unknown Domain Cloud Collaborative Query function (referred to as "Cloud Query"), which retains the original network deployment while using real-time cloud queries to assess the risk status of these unknown domains. This expands the botnet prevention's

signature database by integrating with CloudVista, enhancing DNS traffic analysis and malicious domain control capabilities. This solution can effectively intercept risky DNS traffic at the internet egress, thereby protecting internal network hosts from potential threats.

Typical Application Scenario

The firewall is deployed as a gateway at the internet border egress, combined with CloudVista, to send unknown domain data to the cloud for risk status verification. The function collaborates with the botnet prevention function's domain signature database to analyze the outbound DNS traffic:

- For compliant domain request traffic, it allows;
- For risky domain request traffic, it discards and blocks.



Configuring Unknown Domain Cloud Collaborative Query

Notes: The Unknown Domain Cloud Collaborative Query (Cloud Query) function is controlled by the Botnet Prevention license. When this license expires, the function will be disabled.

Before you start:

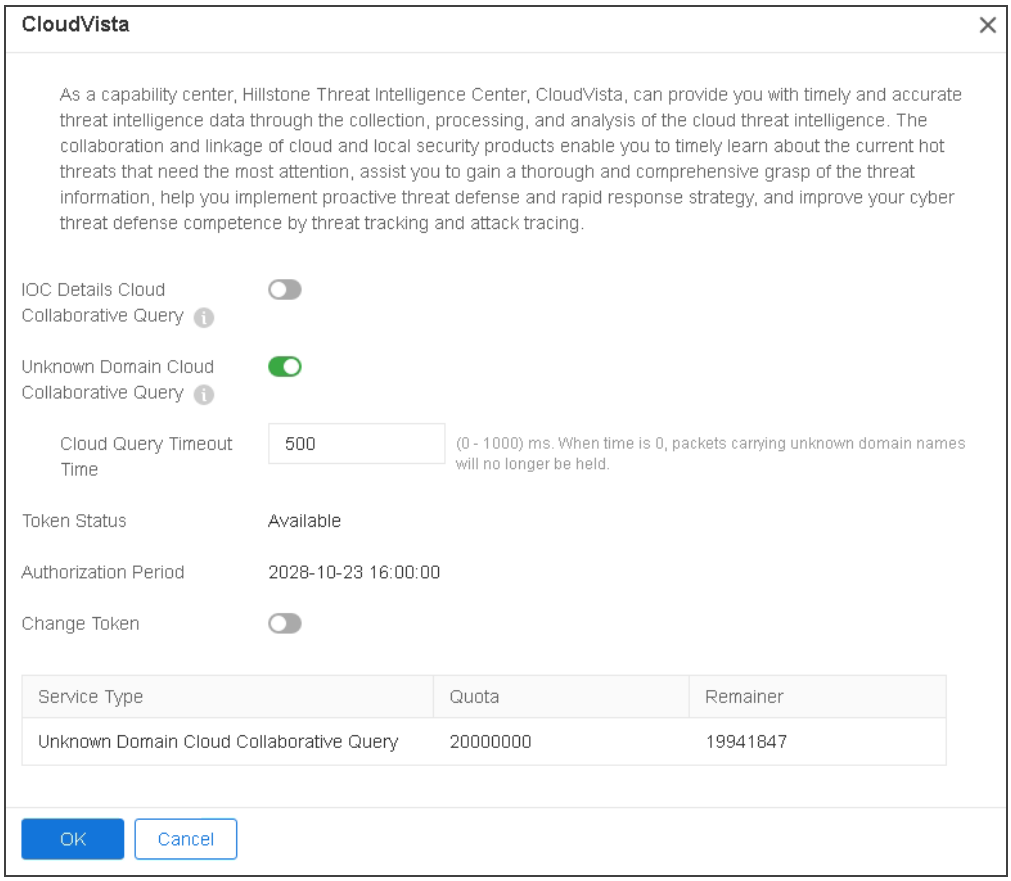
- Read the introduction to the Unknown Domain Cloud Collaborative Query function
- Install the Botnet Prevention license.
- Connecting to Hillstone Cloud Service Platform

To use the Unknown Domain Cloud Collaborative Query (Cloud Query) function, take the following steps:

1. Enabling Unknown Domain Cloud Collaborative Query
2. Configuring Botnet Prevention
3. Querying the Cloud Query Results by IP/Domain/URL
4. (Optional)Clearing Cloud Query Cached Data

Enabling Unknown Domain Cloud Collaborative Query

Select **System > Connecting to Hillstone Cloud Service Platform**. Then, click **CloudVista**.



Step 1: Enable Unknown Domain Cloud Collaborative Query

Turn on the switch next to **Unknown Domain Cloud Collaborative Query** to enable this function. By default, this function is disabled.

Step 2: Obtain the token

When you use the Unknown Domain Cloud Collaborative Query function, you need to specify the token for validation. The cloud provides available query services based on the token, which corresponds to the Hillstone cloud service account that connects to the cloud platform. To obtain the token, take the following steps:

1. Visit https://ti.hillstonenet.com.cn/.
2. Click **Login** to go to the Hillstone Cloud Service login page. Then, use the Hillstone Cloud Service account to log in to the cloud platform.
3. Return to CloudVista. Click the username in the upper-right corner and select **Authorization Management** from the drop-down list.
4. On the page that appears, copy the token displayed in the **API Key** field.

Step 3: Specify the token of Unknown Domain Cloud Collaborative Query

After you enable Unknown Domain Cloud Collaborative Query, specify the obtained token:

1. Enter the token in the **Token** field, which needs to be 64 characters in length.
2. If connected successfully, the status in **Token Status** will display "Available" or "Unavailable". When the Unknown Domain Cloud Collaborative Query function is not enabled, "unavailable" is displayed. In **Authorization Period**, the validity period of the token is displayed.
3. When you edit the configuration, you can see the Change Token function. When enabled, the **Token** field is displayed. To change the token, enter a new one.

Step 4: View the unknown domain query quota/the number of remaining queries

When the Unknown Domain Cloud Collaborative Query function is enabled and the correct token is used to connect to CloudVista, you can view the unknown domain query quota of the current account and the number of remaining queries. By default, the query quota of each account is 10000/day.



Notes: When the quota is exhausted, the device no longer performs unknown domain query on the cloud. To apply for a higher query quota, contact staff from Hillstone Networks.

Step 5: Configure Cloud Query timeout period

After enabling the Unknown Domain Cloud Collaborative Query function, the system will upload unknown domains of the Botnet Prevention function to the cloud for further query, and then handle traffic based on the verification results. The cloud-based verification results can be cached on the device (which can be viewed in Cloud Cache), and is used for subsequent domain detection. During the upload of domain query, the system temporarily suspends forwarding packets containing unknown domains. The maximum duration for suspension is the cloud query timeout period, which is 500 ms by default.

- If the cloud returns the risk status within the cloud query timeout period, the system performs the corresponding action (continue forwarding or drop) based on the cloud query results of unknown domain:
    - Blacklist: Follow the botnet prevention rule;
    - Whitelist/Unknown: Continue forwarding the packets.
- If no cloud-based query results are returned within the cloud query timeout period, packets containing unknown domains will be forwarded.

To configure the Cloud Query timeout period, take the following steps:

1. Keep the default value of 500 ms if no changes are needed.
2. To enter a custom timeout period, enter a value between 0-1000 ms in the Cloud Query Timeout Time field.

Step 6: Complete the configuration

Click OK.

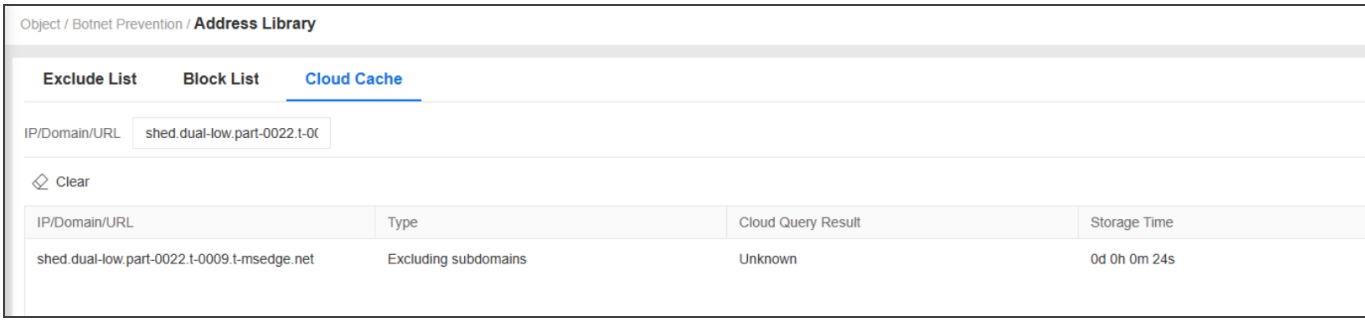
Querying the Cloud Query Results by IP/Domain/URL

After the device is connected to the Hillstone cloud platform, the cloud will periodically push domain/IP/URL to the device. This data, along with results from unknown domain cloud queries, is stored in the device's "Cloud Cache" for future threat detection of botnet prevention. You can precisely query detailed cloud query results by specifying an IP/domain/URL on the **Cloud Cache** tab and proceed with relevant operations based on the query results.

Notes: It is essential to use a known and specific domain/IP/URL when performing queries on this tab.

To search for cloud query results by IP/domain/URL, take the following steps:

1. Select **Object** > **Botnet Prevention** > **Address Library**.
2. Click the **Cloud Cache** tab.
3. In the **IP/Domain/URL** search box, enter the precise IP address, domain, or URL, then press Enter. The cache information will display the detailed type, cloud query result, and storage time in the list below.



4. View cloud query results of the unknown domain. Different actions can be taken based on the cloud query results for unknown domains:
   - **Blacklist**: If the **Cloud Query Result** is **Blacklist**, traffic associated with the domain will be processed based on the botnet defense rules configured in the system. If the domain is determined to be a false positive or the traffic is considered safe to allow, the domain can be added to the custom exception list. To do this, click **Add to exclude list** in the **Operation** column. Once added, any traffic matching this IP address, domain, or URL will no longer be controller by the botnet defense function.
   - **Whitelist/Unknown**: If the **Cloud Query Result** is **Whitelist** or **Unknown**, the traffic will be allowed by default.

5. View the storage duration for cached unknown domains. The maximum storage duration is 24 hours. Once a domain in the cloud cache reaches 24 hours, it is automatically deleted from the device.

Clearing Cloud Query Cached Data

Cloud query cached data is automatically cleared when the device is restarted. In certain scenarios, such as releasing device memory or after a traffic switch, you may need to manually clear all cloud query cached results stored on the device. To do this, take the following steps:

1. Select **Object** > **Botnet Prevention** > **Address Library**.
2. Click the **Cloud Cache** tab.
3. Click **Clear**. In the tips message, click **OK**.

Cloud-Based DNS Security Detection

Introduction

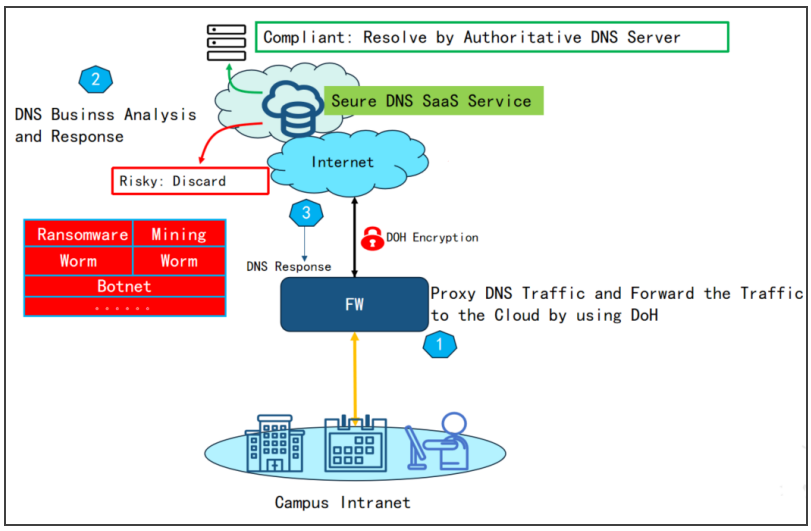
In traditional DNS resolution, packets are transmitted by using unencrypted DNS protocols (such as UDP). Attackers can exploit this by using man-in-the-middle techniques to tamper with DNS traffic, posing significant security threats to organizations.

The system provides the Cloud-Based DNS Security Detection function that maintains the existing network deployment while integrating with a secure DNS SaaS service. This function forwards DNS traffic from the internal network by using DoH (DNS over HTTPS) to the cloud for domain name resolution, ensuring the integrity and confidentiality of the resolution process. In addition, the cloud leverages its extensive threat intelligence to identify and block risky domains or IP addresses, effectively safeguarding internal network hosts.

Typical Application Scenario

The firewall is deployed as a gateway at the internet border egress. After integrating with the secure DNS SaaS service, it proxies internal network's DNS traffic and forwards the traffic to the

cloud by using DoH. While performing domain name resolution, the cloud leverages extensive threat intelligence to identify and block risky domains or IP addresses. Compliant DNS response packets are returned to the firewall, while malicious domains are discarded.



Configuring Cloud-Based DNS Security Detection

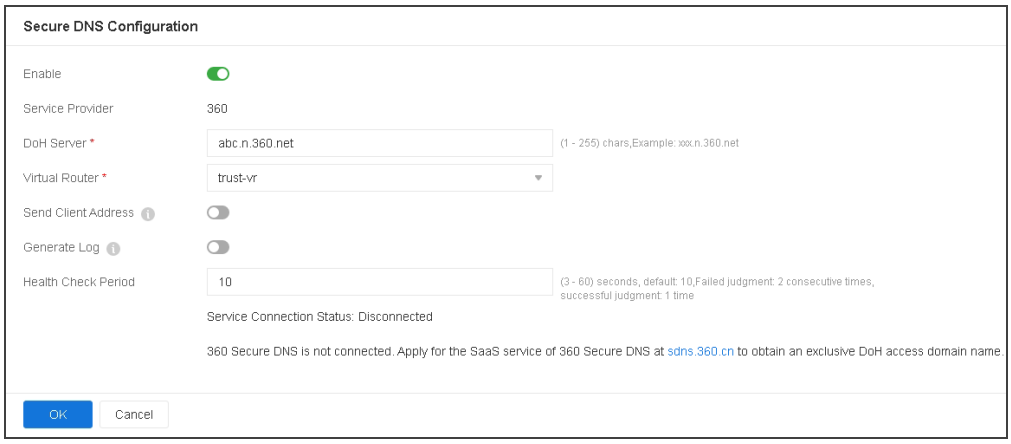
Before you begin

- Read introduction to cloud-based DNS security detection
- Visit sdns.360.cn to apply for the Secure DNS SaaS service.

To configure cloud-based DNS security detection, take the following steps:

1. Select **Configuration Management** > **Network Configuration** > **DNS** > **Secure DNS Configuration**.

2. Click **Enable**.



Option	Description
Service Provider	Displays the name of the DoH server provider.
DoH Server (required)	Enter the domain name of the DoH access server in the format "xxx.n.360.net". Note: Apply for the Secure DNS SaaS service at dns.360.cn to obtain the DoH server domain name first.
Virtual Router (required)	Select the virtual router to which the DoH server belongs from the drop-down list.
Sent Client Address	Click the button to upload the obtained client IP address to the server provider for maintenance. By default, this function is enabled.
Generate Log	Click the button to generate a threat log when you request resolution of a domain deemed a threat through the DNS proxy. By default, this function is disabled.

Option	Description
Health Check Period	Specifies the interval for sending DNS health check packets to the DoH server, ranging from 3 to 60 seconds. The default value is 10 seconds. After configuration, if two consecutive health checks fail, the system will switch the Secure DNS service to Inactive. While in the Inactive state, health checks will still be sent, and the status will immediately switch to Active once a successful check occurs.

3. Click **OK**.

Chapter 13 Monitor

The monitor section includes the following functions:

- "Monitor" on Page 1504: The Monitor function statistically analyzes the devices and displays the statistics in a bar chart, line chart, tables, and so on, which helps the users have information about the devices.
- "Reporting" on Page 1609: Through gathering and analyzing the device traffic data, traffic management data, threat data, monitor data and device resource utilization data, the function provides the all-around and multi-demensional staticstcs.
- "Logging" on Page 1568: Records various system logs, including system logs, threat logs, session logs, NAT logs.
- "NetFlow" on Page 1624: Collects user's ingress traffic according to the NetFlow profile, and send it to the server with NetFlow data analysis tool, so as to detect, monitor and charge traffic.

Monitor

System can monitor the following objects.

- **User Monitor**: Displays the application statistics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month) The statistics include the application traffic and applications' concurrent sessions.
- **Device Monitor**: Displays the device statistics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month), including the total traffic, CPU/memory status, sessions and hardware status.

- **Keyword Block**: If system is configured with "File Content Filter" on Page 1037, "Web Content" on Page 1042, "Email Filter" on Page 1054, "Web Posting" on Page 1048, the pre-defined stat-set of Keyword Block can gather statistics on the file content keyword, Web keyword, Web keywords, email keywords, posting keywords and users/IPs.
- **Locking User**: Displays the information of locked users, including user name, the time when the user is locked, the period how long the user have been locked and available action.
- **Locking IP**: Displays the information of locked IP, including IP address, the time when the IP is locked, the period how long the IP have been locked and available action.
- **Monitor Configuration**: Enable or disable some monitor items as needed.



Notes: If IPv6 is enabled, system will count the total traffic/sessions/AD/URLs/applications of IPv4 and IPv6 address. Only User Monitor/Application Monitor/Cloud Application Monitor/Device Monitor/URL Hit/Application Block/User-defined Monitor support IPv6 address.

User-defined Monitor

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

A user-defined stat-set provides a more flexible approach to view the statistics. You can view the statistics as needed. The statistical data may vary in the data types you have selected.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

The IP type-based statistical information table.

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
No direction	Initiator	Statistics on the traffic of the initiator's IP	Statistics on the session number of the initiator's IP	Statistics on the new sessions of the initiator's IP	Statistics on the URL hit count of the initiator's IP	Statistics on the keyword block count of the initiator's IP	Statistics on the application block count of the initiator's IP
	Responder	Statistics on the traffic of the responder's IP	Statistics on the session number of the responder's IP	Statistics on the new sessions of the responder's IP			
	Belong to zone	Statistics on the traffic of an IP that belongs to a specific security zone	Statistics on the session number of an IP that belongs to a specific security zone	Statistics on the new sessions of an IP that belongs to a specific security zone			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	Not belong to zone	Statistics on the traffic of an IP that does not belong to a specific security zone	Statistics on the session number of an IP that does not belong to a specific security zone	Statistics on the new sessions of an IP that does not belong to a specific security zone			
	Belong to interface	Statistics on the traffic of an IP that belongs to a specific interface	Statistics on the session number of an IP that belongs to a specific interface	Statistics on the new sessions of an IP that belongs to a specific interface			
	Not belong to interface	Statistics on the traffic of an IP that does not belong to a specific interface	Statistics on the session number of an IP that does not belong to a specific interface	Statistics on the new sessions of an IP that does not belong to a specific interface			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
Bi-directional	Initiator	Statistics on the inbound/outbound traffic of the initiator's IP	Statistics on the number of received/sent sessions of the initiator's IP	Statistics on the new received/sent sessions of the initiator's IP	Statistics on the URL hit count of the initiator's IP	Statistics on the keyword block count of the initiator's IP	Statistics on the application block count of the initiator's IP
	Responder	Statistics on the inbound and outbound traffic of the responder's IP	Statistics on the number of received and sent sessions of the responder's IP	Statistics on the new received and sent sessions of the responder's IP			
	Belong to zone	Statistics on the inbound and outbound traffic of an IP that belongs to a specific security zone	Statistics on the number of received and sent sessions of an IP that belongs to	Statistics on the new received and sent sessions of an IP that belongs to			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
			a specific security zone	a specific security zone			
	Not belong to zone	Statistics on the inbound and outbound traffic of an IP that does not belong to a specific security zone	Statistics on the number of received and sent sessions of an IP that does not belong to a specific security zone	Statistics on the new received and sent sessions of an IP that does not belong to a specific security zone			
	Belong to interface	Statistics on the inbound and outbound traffic of an IP that belongs to a specific interface	Statistics on the number of received and sent sessions of an IP that belongs to a specific interface	Statistics on the new received and sent sessions of an IP that belongs to a specific interface			
	Not belong	Statistics on	Statistics	Statistics			

Direction	Condition	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	to interface	the inbound and outbound traffic of an IP that does not belong to a specific interface	on the number of received and sent sessions of an IP that does not belong to a specific interface	on the new received and sent sessions of an IP that does not belong to a specific interface			

The interface, zone, user, application, URL, URL category, VSYS type-based statistical information table.

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
Zone	No direction	Statistics on the traffic of the specified security zones	Statistics on the session number of the specified security zones	Statistics on the new sessions of the specified security zones	Statistics on the URL hit count of the specified security zones	N/A	N/A
	Bi-dir-	Statistics	Statistics	Statistics			

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
	ectional	on the inbound and outbound traffic of the specified security zones	on the number of received and sent sessions of the specified security zones	on the new received and sent sessions of the specified security zones			
Interface	No direction	Statistics on the traffic of the specified interfaces	Statistics on the session number of the specified interfaces	Statistics on the new sessions of the specified interfaces	Statistics on the URL hit count of the specified interfaces	N/A	N/A
	Bi-directional	Statistics on the inbound and outbound traffic of the specified interfaces	Statistics on the number of received and sent sessions of the specified interfaces	Statistics on the new received and sent sessions of the specified interfaces			
Application	N/A	Statistics	Statistics	Statistics	N/A	N/A	Statistics

Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
		on the traffic of the specified applications	on the session number of the specified applications	on the new sessions of the specified applications			on the block count of the specified applications
User	No direction	Statistics on the traffic of the specified users	Statistics on the session number of the specified users	Statistics on the new sessions of the specified users	Statistics on the URL hit count of the specified users	Statistics on the keyword block count of the specified users	Statistics on the application block count of the specified users
	Bi-directional	Statistics on the inbound and outbound traffic of the specified users					
URL	N/A	N/A	N/A	N/A	Statistics on the hit count of	N/A	N/A

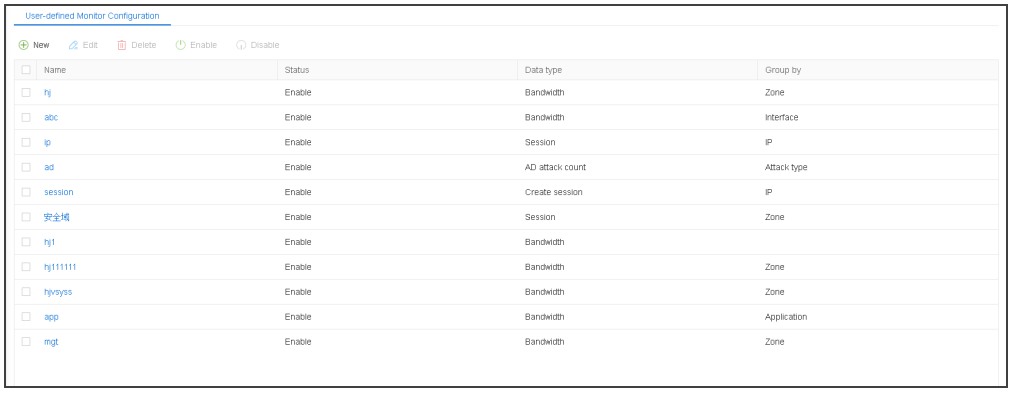
Group by	Direction	Data type					
		Traffic	Session	Ramp-up rate	URL hit count	Keyword block count	Application block count
					the specified URLs		
URL Category	N/A	N/A	N/A	N/A	Statistics on the hit count of the specified URL categories	N/A	N/A
VSYS	N/A	Statistics on the traffic of the specified VSYSs	Statistics on the session number of the specified VSYSs	Statistics on the new sessions of the specified VSYSs	Statistics on the URL hit count of the specified VSYSs	N/A	N/A

You can configure a filtering condition for the stat-set to gather statistics on the specified condition, such as statistics on the session number of the specified security zone, or the traffic of the specified IP. The system supports up to 32 filters for each stat-set, among which the number of filters for each type of the user, user group and role filters cannot exceed 8. If multiple filters configured for the same stat-set belong to the same type, then the logical relationship among these conditions will be OR; if they belong to different types, the logical relationship among these conditions will be AND.

The filtering conditions supported table.

Type	Description
filter zone	Data is filtered by security zone.
filter zone zone-name ingress	Data is filtered by ingress security zone.
filter zone zone-name egress	Data is filtered by egress security zone.
filter interface	Data is filtered by interface.
filter interface if-name ingress	Data is filtered by ingress interface.
filter interface if-name egress	Data is filtered by egress interface.
filter application	Data is filtered by application.
filter ip	Data is filtered by address entry.
filter ip add-entry source	Data is filtered by source address (address entry).
filter ip add-entry destination	Data is filtered by destination address (address entry).
filter ip A.B.C.D/M	Data is filtered by IP.
filter ip A.B.C.D/M source	Data is filtered by source IP.
filter ip A.B.C.D/M destination	Data is filtered by destination IP.
filter user	Data is filtered by user.
filter user-group	Data is filtered by user group.
filter role	Data is filtered by user role.
filter service	Data is filtered by service.

Click **Monitor>User-defined Monitor**.

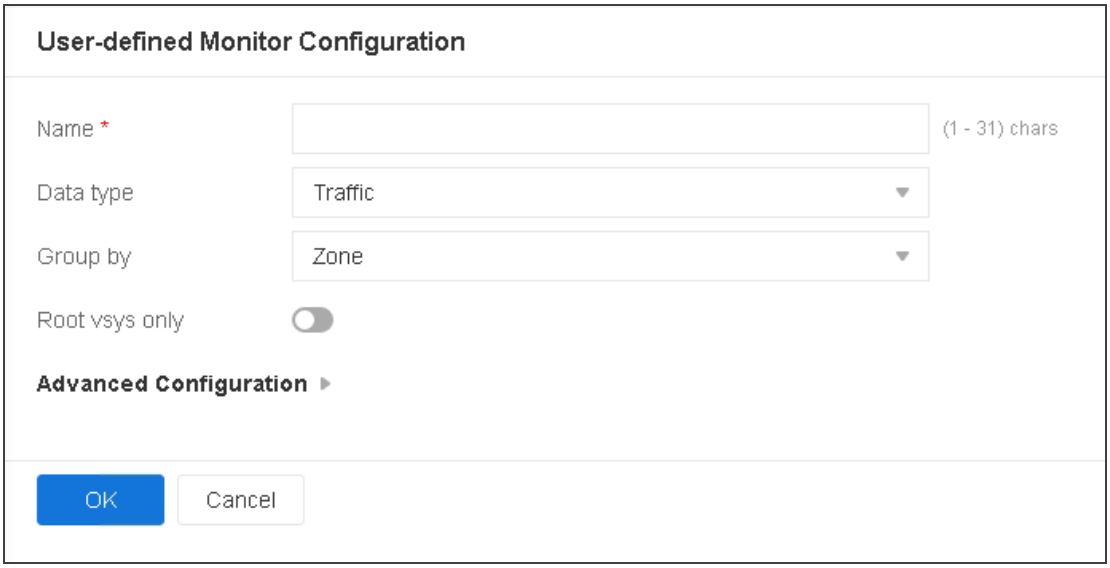


- Click **New**. For more information, see Creating_a_User-defined_Stat-set
- Click the user-defined stat-set name link. For more information, see Viewing_User-defined_Stat-set_Statistics.

Creating a User-defined Stat-set

To create a user-defined stat-set, take the following steps:

1. Click **Monitor > User Defined Monitor**.
2. Click **New**.



Option	Description
Name	Type the name for the stat-set into the Name box.
Data Type	Select an appropriate data type from the Data type list.
Group by	Select an appropriate grouping method from the Group by list.
Root vsys only	If you only want to perform the data statistics for the root VSYS, click the **Enable** button. This button will take effect when the data type is Traffic, Session, Ramp-up rate, or URL hit. If the data grouping method is configured to VSYS, this button will be unavailable.
Advanced Configuration	To configure a filtering condition, expand Advanced Configuration. In the Advanced Configuration page, select a filter condition from the Type drop-down list. For more details about this option, see The_filtering_conditions_supported_table.

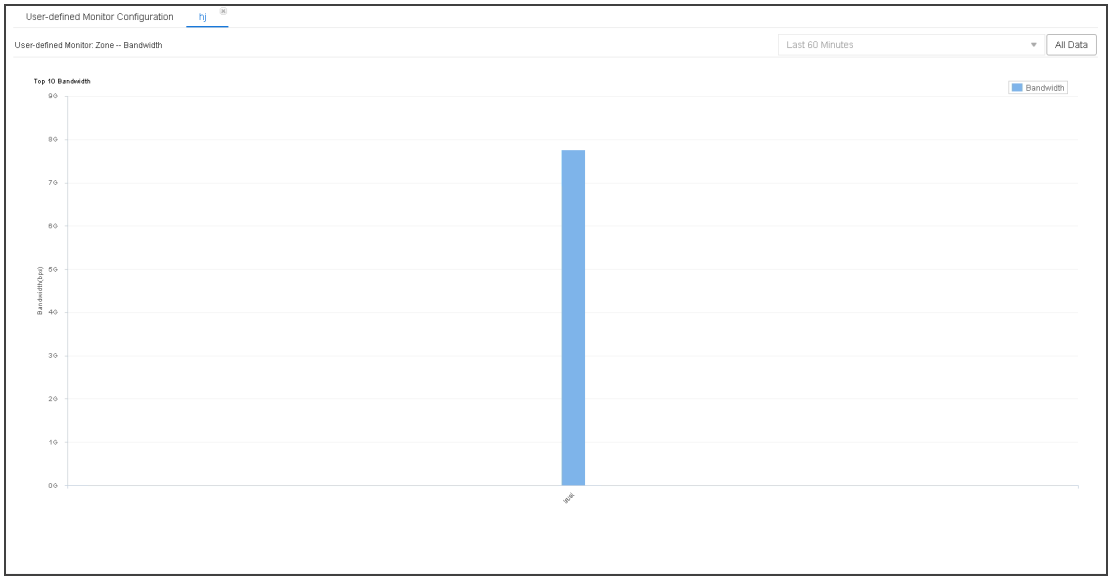
3. Click **OK** to save your settings . The configured stat-set will be displayed .

Notes: You need to pay attention to the following when configure a stat-set.

- The URL hit statistics are only available to users who have a URL license.
- If the Data type is Traffic, Session, Ramp-up rate, Virus attack count, Intrusion count or URL hit count, then the Filter should not be Attack log.
- If the Data type is URL hit count, then the Filter should not be Service.
- System will hide unavailable options automatically.

Viewing User-defined Monitor Statistics

Click the user-defined stat-set name link, and then select the stat-set you want to view.



- Displays the top 10 statistical result from multiple aspects in forms of bar chart.
- View specified historic statistics by selecting a period from the statistic period drop-down list.
- Click **All Data** to view all the statistical result from multiple aspects in forms of list, trend.

  Click **TOP 10** returns bar chart.

Application Monitor

Application monitor displays the statistics of applications, application categories, application sub-categories, application risk levels, application technologies, and application characteristics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month) .The statistics include the application traffic and applications' concurrent sessions.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

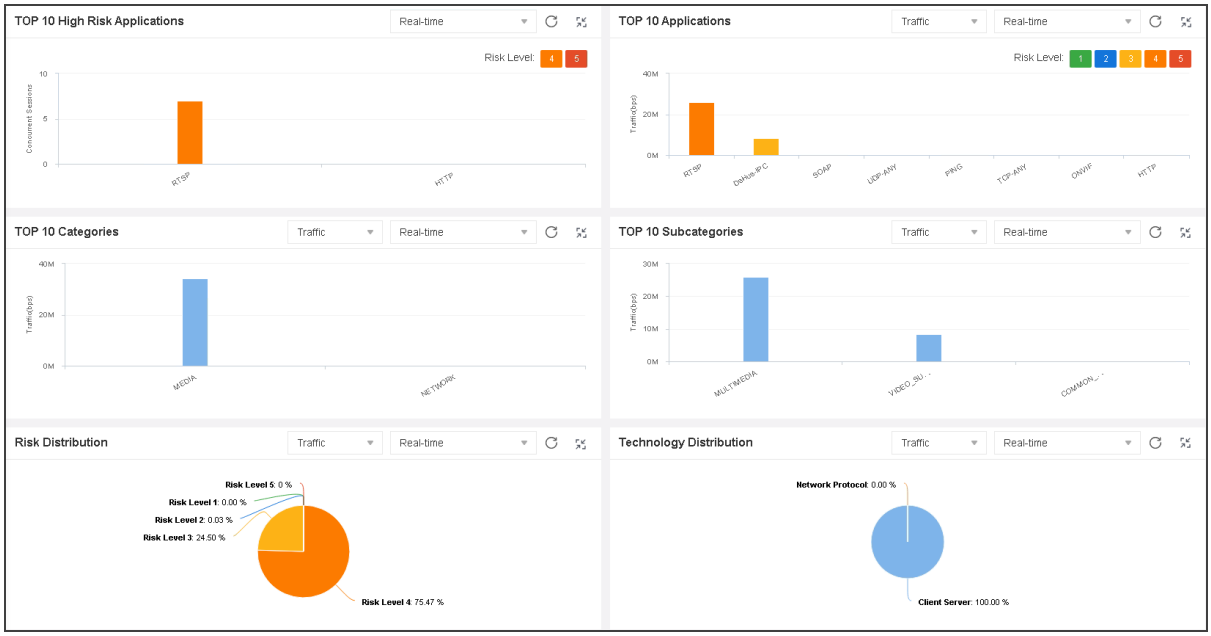
Notes: Non-root VSYS also supports application monitor, but does not support to monitor application group.

Summary

The summary displays the following contents during a specified period:

- The concurrent sessions of top 10 hot and high-risk applications.
- The traffic/concurrent sessions of top 10 applications.
- The traffic/concurrent sessions of top 10 application categories.
- The traffic/concurrent sessions of top 10 application subcategories.
- The traffic/concurrent sessions organized by application risk levels.
- The traffic/concurrent sessions organized by application technologies.
- The traffic/concurrent sessions organized by application characteristics.

Click **Monitor>Application Monitor>Summary**.

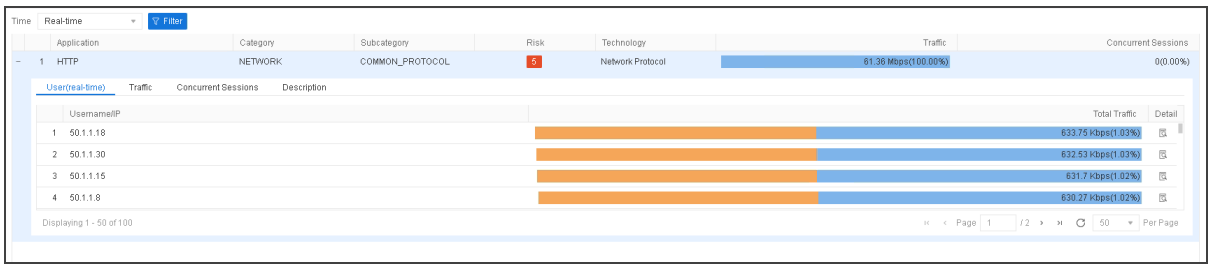


- Select different Statistical_Period to view the statistical information in different periods of time.
- From the drop-down menu, specify the type of statistics: Traffic or Concurrent Sessions.
- Click " " to refresh the monitoring data in this page.

- Click " " to close the current frame.
- Hover your mouse over a bar or a pie graph to view the concrete statistical values of total traffic or concurrent sessions.

Application Details

Click **Monitor > Application Monitor > Application Details**.

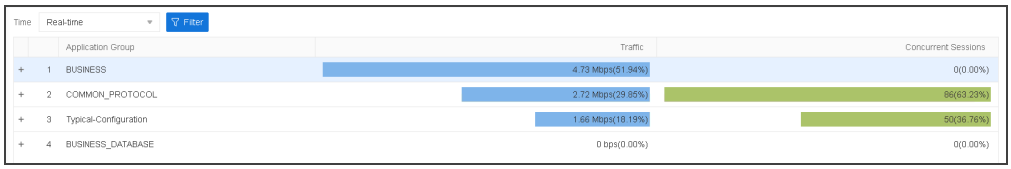


- Click the **Time** drop-down menu to select different Statistical_Period to view the statistical information in that periods of time.
- Click Filter button and select **Application** in the drop-down menu. You can search the desired application by entering the keyword of the application's name in the text field.
- To view the detailed information of a certain application, select the application entry in the list, and click "+".
    - Users(real-time): Select the Users (real-time) tab to displays the detailed information of users who are using the selected application. Click in details column to see the trends of upstream traffic, downstream traffic, total traffic.
    - Traffic: Select the Traffic tab to display the traffic trends of selected application.
    - Concurrent Sessions: Select the Concurrent Sessions tab to display the concurrent sessions trends of the selected application.

- Description: Select the Description tab to displays the detailed information of the selected application.

Group Details

Click **Monitor>Application Monitor>Group Details**.

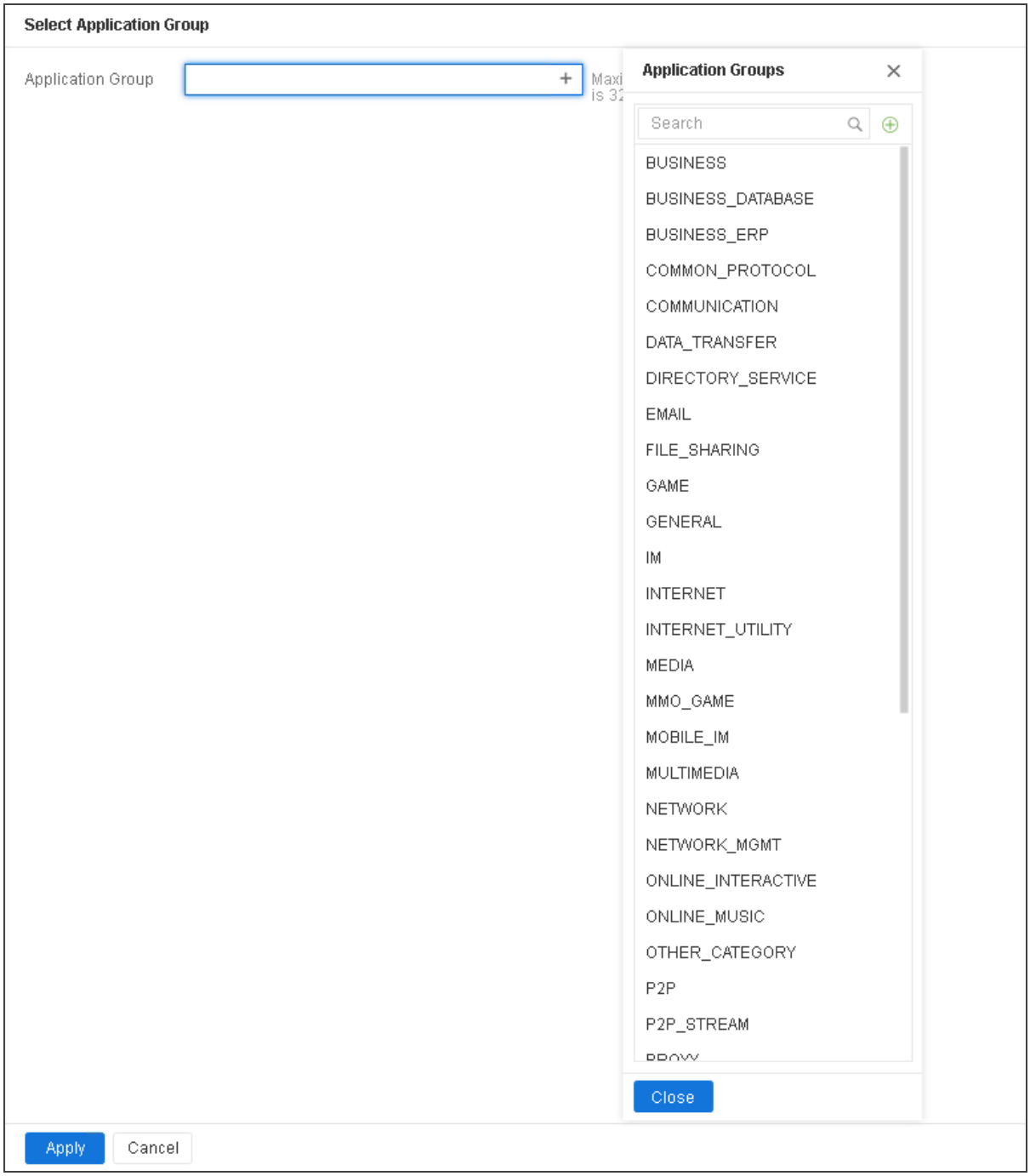


- Click **Time** drop-down menu to select a different Statistical_Period to view the statistical information in that periods of time.
- Click Filter button and select **Application Group** in the drop-down menu. You can search the desired application group by entering the keyword of the application group name in the text field.
- To view the detailed information of a certain application group, select the application group entry in the list, and click "+".
  - User (real-time): Select the Users (real-time)tab to display the detailed information of users who are using the selected application group. Click in details column, you can see the trends of the upstream traffic, downstream traffic, total traffic .
  - Application(real-time): Select the Application(real-time) tab to display the detailed information of applications in use which belongs to the selected application group. Click in details column to see the trends of the upstream traffic, downstream traffic, total traffic of the selected application.
  - Traffic: Select the Traffic tab to display the traffic trends of selected application group.

- Concurrent Sessions: Select the Concurrent Sessions tab to display the concurrent sessions trends of the selected application group.

Select Application Group

Click **Monitor>Application Monitor>Select Application Group**. There are global application groups in the right column.



In this page, you can perform the following actions:

- Click the desired address entry check box to add a new address entry to the left list.
- In the left list, click an address entry to remove it from the list.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click **Real-time** on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

Cloud Application Monitor

This feature may vary slightly on different platforms and not be available in VSYS on a part of platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

A cloud application is an application program that functions in the cloud. It resides entirely on a remote server and is delivered to users through the Internet.

Cloud application monitor page displays the statistics of cloud applications and users within a specified period (realtime, latest 1 hour, latest 1 day, latest 1 month), including application traffic, user number, and usage trend.

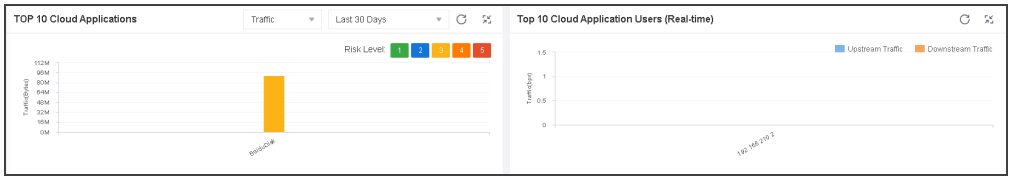
If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Summary

The summary displays the following contents during a specified period:

- Top 10 cloud application rank by traffic/concurrent session number with in a specified period (realtime, latest 1 hour, latest 1 day, latest 1 month).
- Top 10 cloud application user rank by application number/traffic/concurrent session/new session.

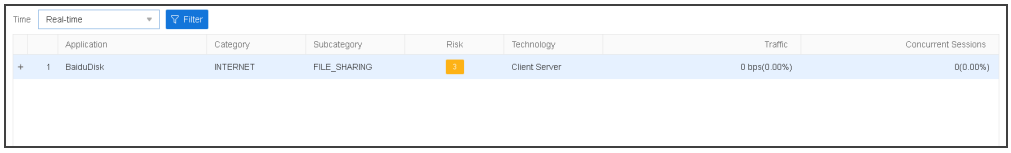
Click **Monitor > Cloud Application Monitor> Summary**.



- By selecting different filters, you can view the statistics of different time period.
- By selecting the drop-down menu of trafficor concurrent sessions, you can view your intended statistics.
- Click the update icon to update the displayed data.
    - Hover your cursor over bar or pie chart to view exact data. Click the **Details** link on hover box, and you will jump to the **Cloud Application Details** page.

Cloud Application Details

Click **Monitor > Cloud Application Monitor>Cloud Application Details**.



- Click the Time drop-down menu to select different time period to view the statistics in that period.
- Click the **Filter** button, and select **Application**. In the new text box, enter the name of your intended application.
- To view the detailed information of a certain application group, select the application group entry in the list and click + before it.
    - User(real-time): Select the Users(real-time) tab to display the detailed information of users who are using the selected application group. Click in details column to see

the trends of the upstream traffic, downstream traffic, total traffic .

- Traffic: Select the Traffic tab to display the traffic trends of selected application.
- Concurrent Sessions: Select the Concurrent Sessions tab to display the concurrent sessions trends of the selected application.
- Description: Select the Description tab to display the detailed description of the selected application.

Statistical Period

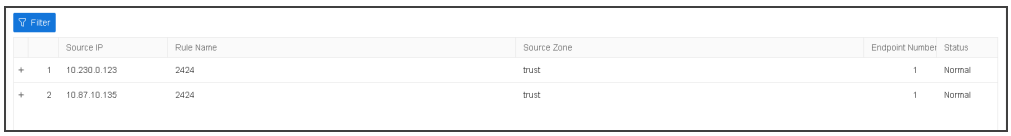
System supports the predefined time cycle and the custom time cycle. Click **Real-time** on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

Share Access Monitor

To detect the users' private behavior of shared access to the Internet, system supports to analyze the User-agent filed of HTTP packet, a share access detect method which is based on the application characteristic. The share access detect page can display the share access information with specified filter condition.

Click **Monitor> Share Access**.



- Click Filter to select the condition in the drop-down list to search for the share access.
- Source IP: Displays the endpoints statistics of the specified source IP (IPv4 or IPv6).
- Rule Name: Displays the endpoints statistics of the specified share access rule.
- Source Zone: Displays the endpoints statistics of the specified source zone.
- Endpoint Number: Displays the endpoints statistics of the specified endpoint number.
- Status: Displays the endpoints statistics of the specified status, including the normal status, logging status, warning status, and blocking status.

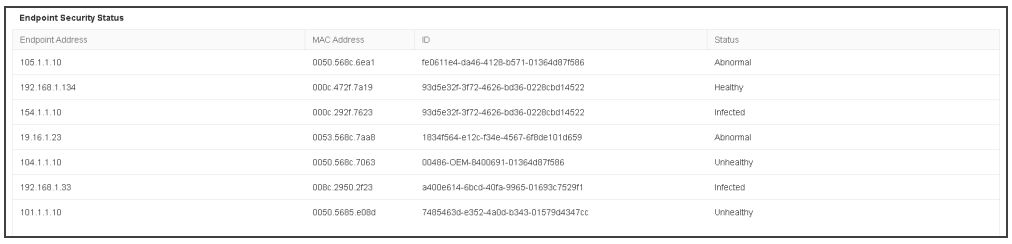
Move the mouse to **Endpoint Number** list, click + button, you will view the list of **Endpoint info** and **First Detection Time**.



End Point Monitor

If system is configured with "Configuring End Point Security Control Center Parameters" on Page 1458, the endpoint detect page displays the endpoint data information list synchronized with the endpoint security control center.

Click **Monitor** > **End Point Monitor**.



User Quota Monitor

After the "Traffic Quota" on Page 1255 function is configured, the user quota detect page displays the user traffic quota statistics list, including the user's daily/ monthly quota, daily/ monthly used traffic value, the user group, and the corresponding traffic quota rule name.



- Type the user name into the **User Name** text box to filter the user traffic quota statistics for the specified name.
- Click in the **Clear/Reset** column of the list to clear the selected user daily used traffic.
- Click in the **Clear/Reset** column of the list to clear the selected user monthly used traffic.
- Click in the **Clear/Reset** column of the list to reset all used traffic for the selected user.
- Click **Clear All Used Traffic** to clear all used traffic of all users in the list.

Application Block

If system is configured with "Security Policy" on Page 1089 the application block can gather statistics on the applications and user/IPs.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Summary

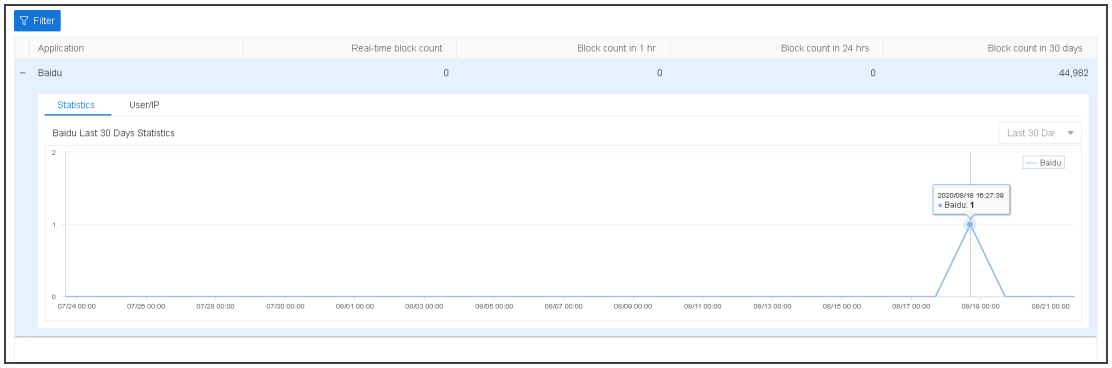
The summary displays the application block's statistics on the top 10 applications and top 10 user-/IPs. Click **Monitor>Application Block> Summary**.



- Select a different Statistical_Period to view the statistical information in that period of time.
- Hover your mouse over a bar to view the block count on the applications and user/IPs.
- Click to switch between the bar chart and the pie chart.
- Click to close the chart.
- Click at the top-right corner of every table and enter the corresponding details page.

Application

Click **Monitor>Application Block> Application**.



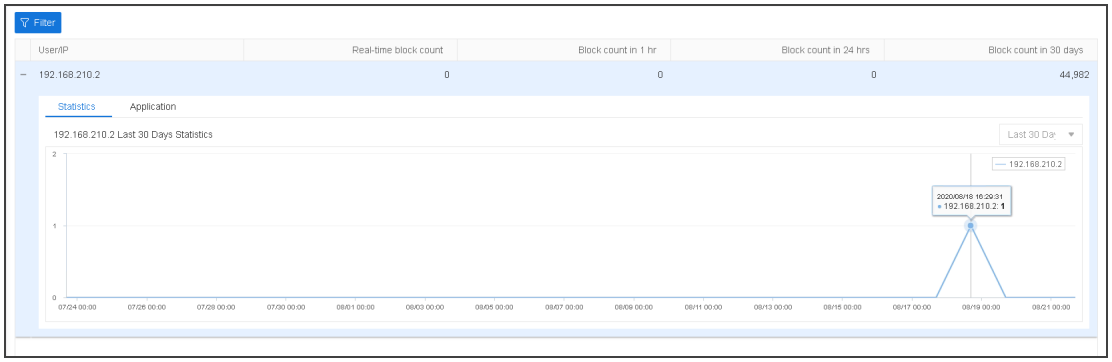
- The applications and detailed block count are displayed in the list.
- To view the corresponding information of application block on the applications and user/IPs, select the application entry in the list, and click "+".
    - Statistics: Displays the block count statistics of the selected application, including the real-time statistics and statistics for the latest 1 hour, 24 hours and 30 days.

- User/IP: Displays the user/IPs that are blocked from the selected application. Click a user/IP in the list to display the corresponding block count statistics in the curve chart below. Click to jump to the corresponding user / IPs page.

- Click Filter to select the condition in the drop-down list. You can search the application block information by entering the keyword of the application name.
- Click to refresh the real-time data in the list.

User/IP

Click **Monitor>Application Block> User/IP**.



- The user/IP and detailed block count are displayed in the list.
- Click a user/IP in the list to display the corresponding block count statistics in the curve chart below. Click to jump to the corresponding user / IPs page.
- Click Filter to select the condition in the drop-down list. You can search the users/IPs information.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click (Real-time) on the top right corner of each tab to set the time cycle.

- Real-time: Displays the statistical information within the realtime.
- Last Hour: Displays the statistical information within the latest 1 hour.
- Last Day: Displays the statistical information within the latest 1 day.
- Last Month: Displays the statistical information within the latest 1 month.

iQoS Monitor

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

When the iQoS policy is configured and the function of iQoS is enabled, you can view the real-time traffic details or traffic trends of pipes and sub-pipes in Level-1 Control or Level-2 Control.



Notes: The iQoS monitor function is controlled by license, To use the function, install the iQoS license.For more information on license, please refer to the License .

- Click the "Edit" button to edit the selected pipe.
- Mouse over the bar of the Traffic columns to see the forward and backward traffic of the pipe.

Device Monitor

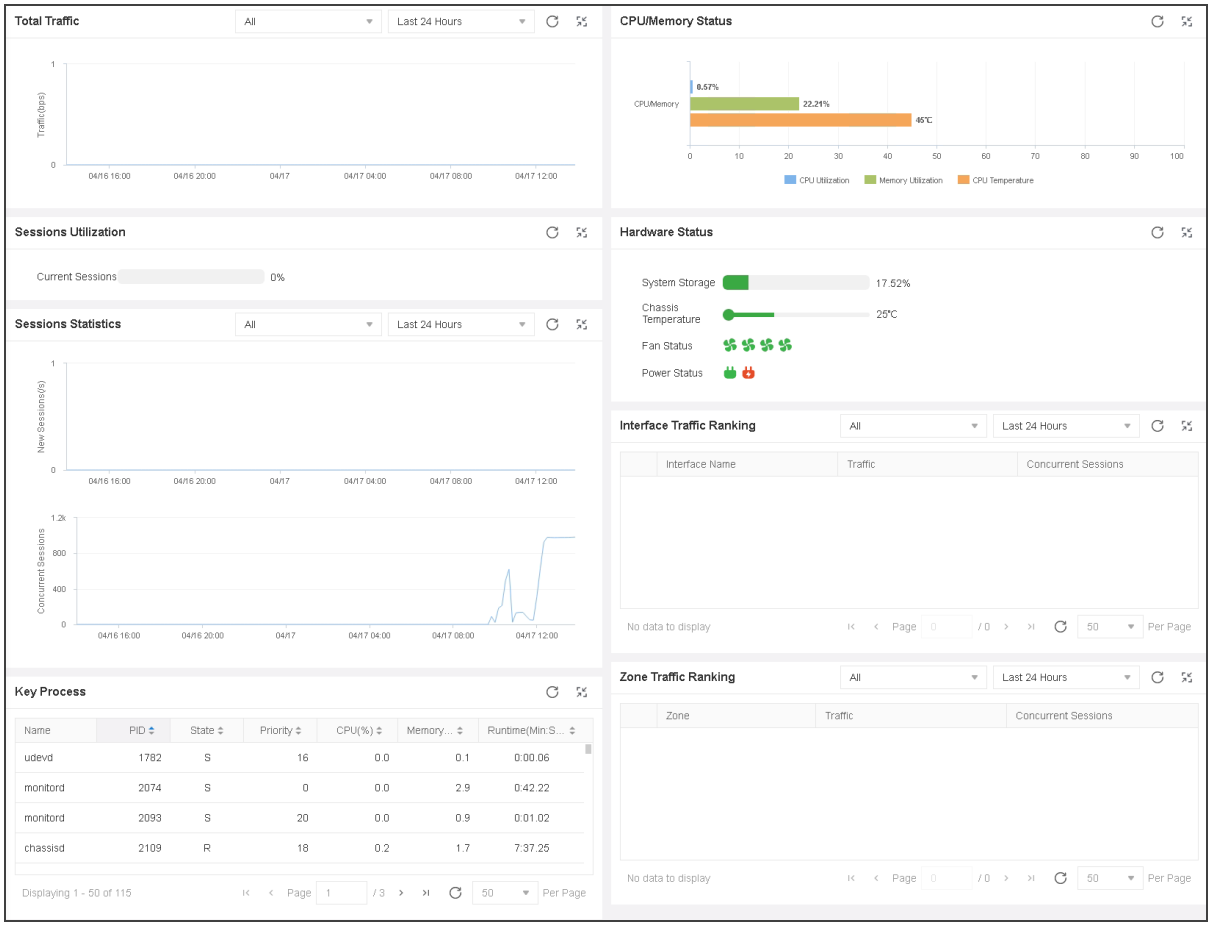
This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

The Device page displays the device statistics within the specified period, including the total traffic, interface traffic, zone traffic, CPU/memory status, sessions, hardware status and online IP.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Summary

The summary displays the device statistics within last 24 hours. Click **Monitor > Device Monitor > Summary**.



- Total traffic: Displays the total traffic within the specified statistical period.
    - Hover your mouse over the chart to view the total traffic statistics at a specific point in time.
    - Select a different Statistical Period to view the statistical information in that period of time.

- Select the address type from the drop-down list 

to view the IPv4 traffic, IPv6 traffic or total traffic of IPv4 and IPv6.

- Interface Traffic Ranking: Displays the upstream traffic, downstream traffic, total traffic and concurrent sessions of interface within the specified statistical period by rank.
  - Select the address type from the drop-down list 

to view the IPv4 traffic, IPv6 traffic or total traffic of IPv4 and IPv6.
  - Select a different Statistical Period to view the statistical information in that period of time.
  - Click the interface name to view the Detailed Information.
  - If IPv6 is enabled, the interface traffic will show the traffic of IPv4 and IPv6.
- Zone Traffic Ranking: Displays the upstream traffic, downstream traffic, total traffic and concurrent sessions of zone within the specified statistical period by rank.
  - Select the address type from the drop-down list 

to view the IPv4 traffic, IPv6 traffic or total traffic of IPv4 and IPv6.
  - Select a different Statistical Period to view the statistical information in that period of time.
  - Click the zone name to view the Detailed Information.
- Hardware Status: Displays the real-time hardware status, including storage, chassis temperature and fan status.

- System Storage: Displays the current system storage space of the device.
- Data Storage: Displays the current data storage space of the device. Only devices with hard disks support this function.
- Chassis temperature: Displays the current CPU/chassis temperature.
    - Click **Chassis Temperature** for system to display the CPU/chassis temperature trend.
    - Hover your mouse over the chart to view the CPU/chassis temperature statistics at a specific point in time.
    - Select a different Statistical Period to view the statistical information in that period of time.
- Fan status: Displays the operation status of the fan. Green indicates normal, and red indicates error or a power supply module is not used.
- Power Status: Displays the power status of the device. Green indicates that the power module is normal. Red indicates that the power module is faulty or not in use.

- Sessions: Displays the current sessions utilization.
    - From the 

drop-down list, you can select different address types to view the new session rate trend and concurrent session number trend of IPv4, the new session rate trend and concurrent session number of IPv6, and the new session rate trend and concurrent session number trend of IPv4 and IPv6 respectively;
    - Hover you mouse over the chart to view the new session rate and the number of concurrent sessions at the specified point in time;

        - Select a different Statistical Period to view the statistical information in that period of time.

- CPU/memory status: Displays current CPU utilization, memory utilization and CPU temperature statistics.

    - Click legends of **CPU Utilization**, **Memory Utilization** or **CPU Temperature** to specify the histogram statistical objects. By default, it displays statistics of all objects.

    - Hover your mouse over the histogram to view the detailed information about CPU utilization, memory utilization, or CPU temperature.

    - Click Details under **CPU utilization or memory utilization** to view the trend of specified histogram.

        - Hover your mouse over the chart to view CPU utilization or memory utilization statistics at a specific point in time.

        - Select different Statistical Period to view the statistical information in different period of time.

- Key Process: Displays information about key processes on the device, including process name, PID, state, priority, CPU percentage, memory percentage, and runtime.

Statistical Period

System supports the predefined time cycle. The statistical period may vary slightly on different monitored objects. If there is conflict between this guide and the actual page, the latter shall prevail. Select statistical period from the drop-down menu 

at the top right corner of some statistics page to set the time cycle.

- Last 5 Minutes: Displays the statistical information within the latest 5 Minutes.

- Last 15 Minutes: Displays the statistical information within the latest 15 Minutes.

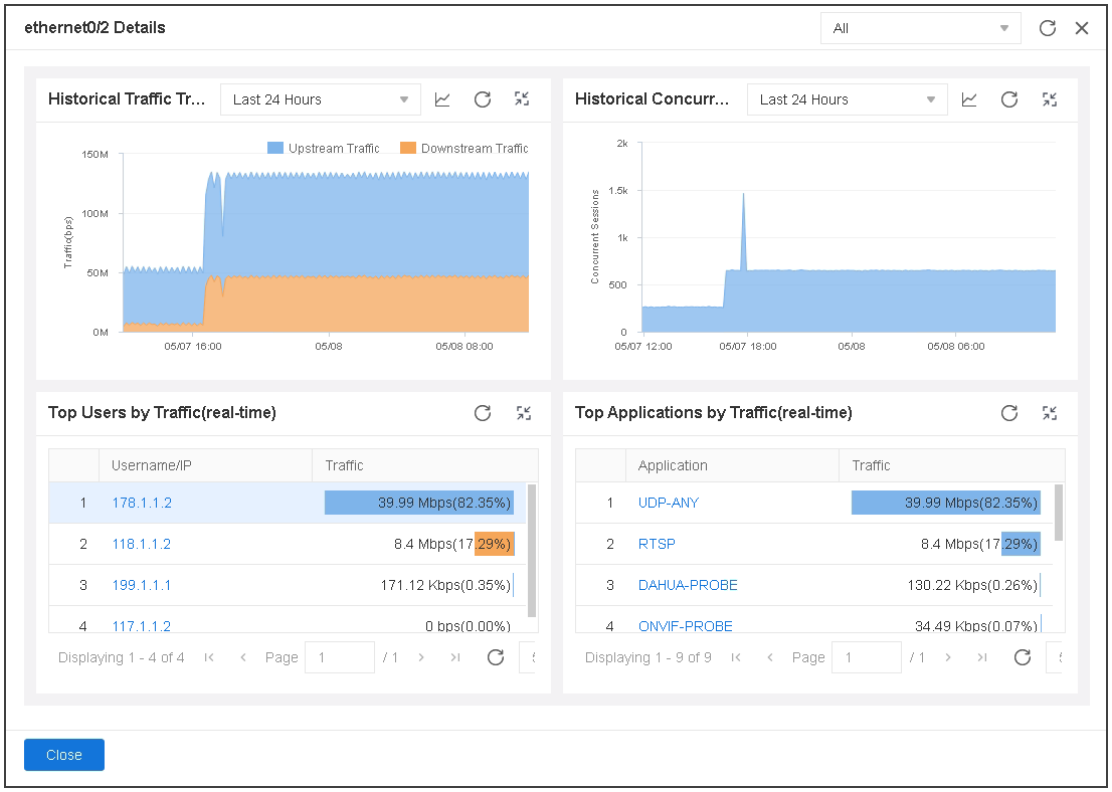
- Custom: Displays the statistical information within the custom period. Click **Custom** to configure the start time and end time.
- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

In the top-right corner, you can set the refresh interval of the displayed data.

Detailed Information

The detailed information page displays detailed statistics of certain monitored objects. In addition, in the detailed information page, hover your mouse over the chart that represents a certain object to view the statistics of history trend and other information.

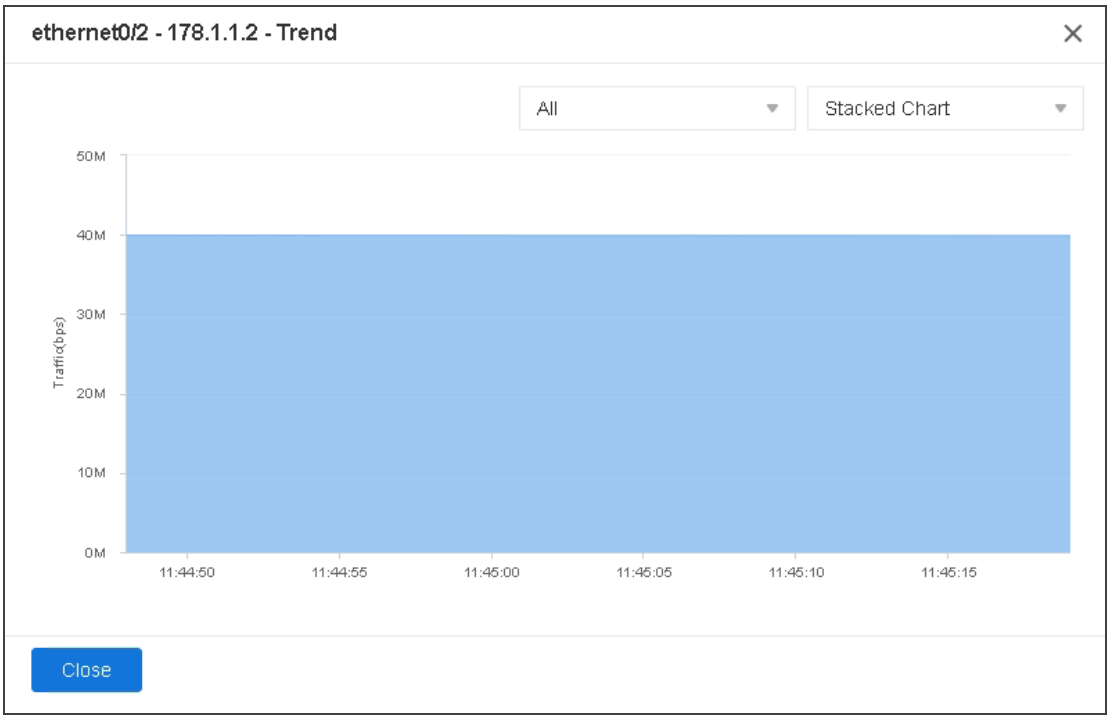
For example, click **ethernet0/2** in the Interface Traffic , and the detailed information of ethernet0/2 appears.



- The drop-down list 

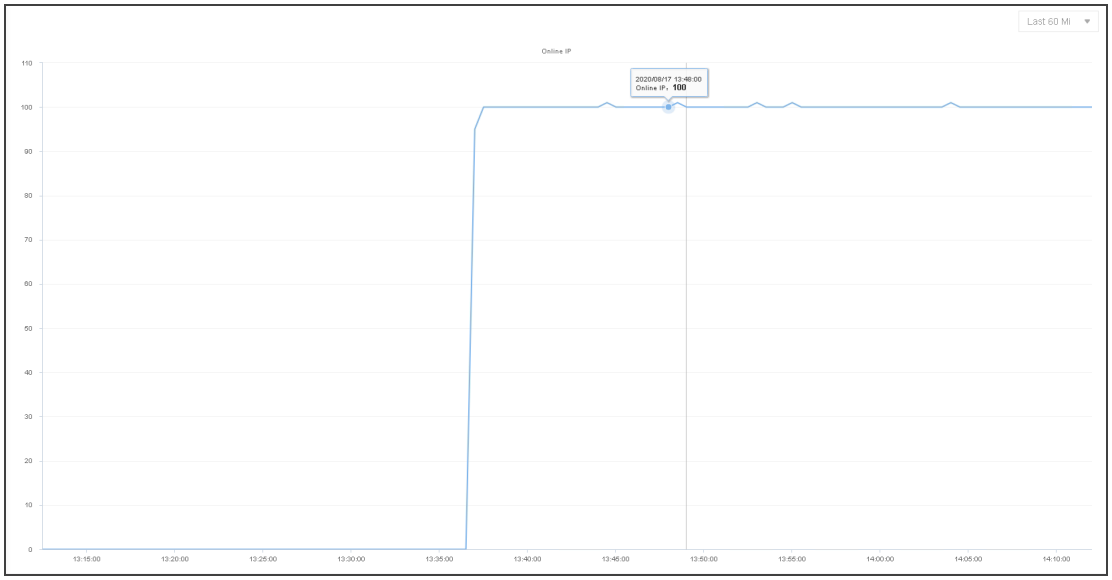
is used to specify the statistical type of interface traffic, including all, IPv4 and IPv6.
- Icon and are used to switch the line chart and stacked chart, which display the history trend of sessions and concurrent sessions.
- In traffic trend section, click legends of **Traffic In** or **Traffic Out** to specify the statistical objects. By default, it displays all statistical objects.
- In the User or Application section, click **Username/IP** or **Application** to display the real-time trend of the specified user or application. For example, the user traffic trend is shown as

below.



Online IP

Click **Monitor>Device>Online IP** to view the historical trend of the number of online users. You can select the statistical period as last 60 minutes, last 24 hours or last 30 days.



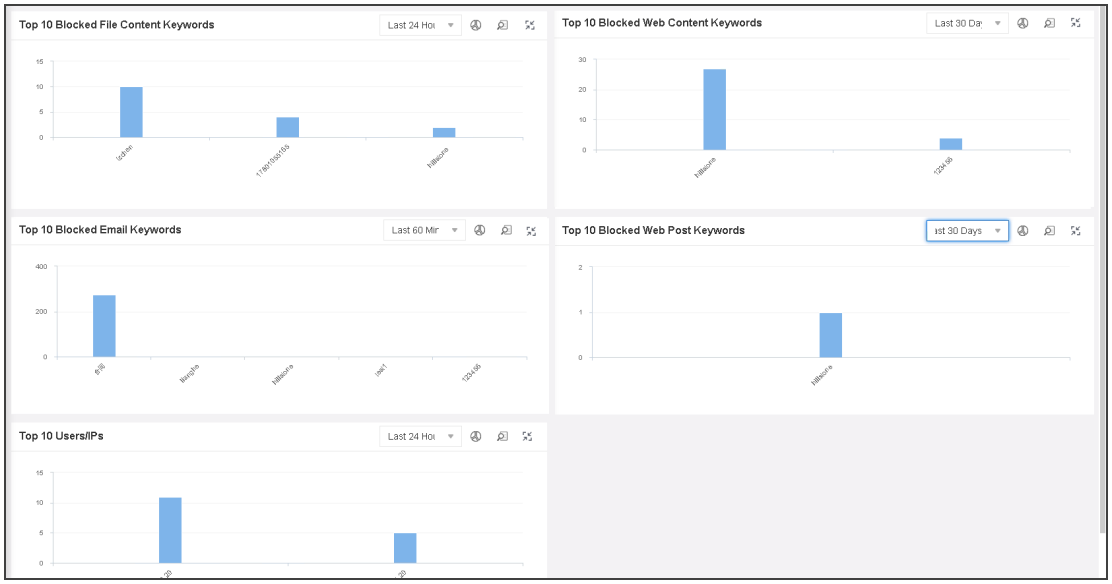
Keyword Block

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

If system is configured with "File Content Filter" on Page 1037, "Web Content" on Page 1042, "Email Filter" on Page 1054, or "Web Posting" on Page 1048, the predefined stat-set of the Keyword Block can gather statistics on the file content keyword, Web keyword, Web keywords, email keywords, posting keywords and users/IPs.

Summary

The summary displays the predefined stat-set of the Keyword Block that can gather statistics on the top 10 blocked file content keywords, the top 10 blocked Web keywords, the top 10 blocked email keywords, the top 10 posting keywords, and the top 10 users/IPs. Click **Monitor > Keyword Block > Summary**.



- Select a different Statistical_Period to view the statistical information in that period of time.
- Hover your mouse over a bar to view the block count on the keywords .

- Click at the top-right corner of every table and enter the corresponding details page.
- Click to switch between the bar chart and the pie chart.

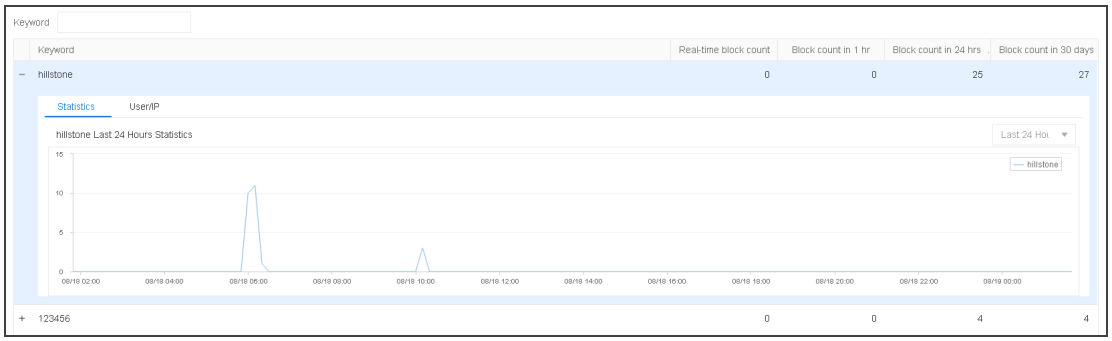
File Content

Click **Monitor>Keyword Block> File Content**.

For a page description, see Web_Content.

Web Content

Click **Monitor>Keyword Block> Web Content**.



- The Web content and detailed block count are displayed in the list below.
- To view the corresponding information of keyword block on the Web content, select the keyword entry in the list.
    - Statistics: Displays the statistics of the selected keyword, including the real-time statistics and statistics for the latest 1 hour, 24 hours and 30 days.
    - User/IP: Displays the user/IPs that are blocked by the selected keyword. Click a user-/IP in the list to display the corresponding block count statistics in the curve chart below. Click to jump to the corresponding user / IPs page.

- Click Filter to select the condition in the drop-down list. You can search the keyword block information by entering the keyword .
- Click to refresh the real-time data in the list.

Email Content

Click **Monitor>Keyword Block> Email Content**.

For a page description, see Web_Content.

Web Posting

Click **Monitor>Keyword Block>Web Posting**.

For a page description, see Web_Content.

User/IP

Click **Monitor>Keyword Block>User/IP**.



- The user/IP and detailed block count are displayed in the list below.
- Click a user/IP in the list to display the corresponding statistics , Web content, Email Content, Web Posting in the curve chart below. Click to jump to the corresponding detail page.

- Click Filter to select the condition in the drop-down list. You can search the users/IPs information .

Statistical Period

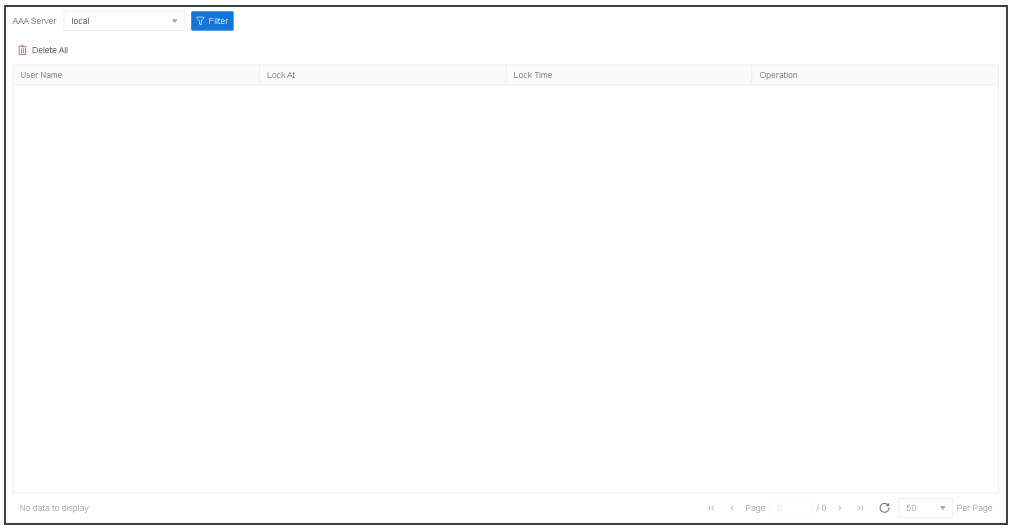
System supports the predefined time cycle and the custom time cycle. Click (Real-time) on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last Hour: Displays the statistical information within the latest 1 hour.
- Last Day: Displays the statistical information within the latest 1 day.
- Last Month: Displays the statistical information within the latest 1 month.

Locking User

After the brute-force cracking defense is configured, the Lock User page will display the information of locked users, including user name, the time when the user is locked, the period how long the user have been locked and available action.

Click **Monitor** > **Lock User**.



- Select a server from the **AAA Server** drop-down list, and the locked user of the server will be displayed in the following list.
- Click  to add filtering conditions and the locked users who meet the conditions will be displayed in the following list.
- Click **Delete** in the Operation column, and the corresponded locked users will be unlocked and deleted.
- Click the **Delete All** button above the list, and all the locked users in the list will be unlocked and deleted.

Notes:

- For how to configure the brute-force cracking defense, refer to AAA server.
- At most 2000 locked users can be displayed in the list. When the threshold is exceeded, the earliest locked user will be unlocked and deleted in the list.

Locking IP

After the brute-force cracking defense is configured, the Lock IP page will display the information of locked IP including IP address, the time when the IP is locked, the period how long the IP have been locked and available action.

Click **Monitor** > **Lock IP**.



- Select a server from the **AAA Server** drop-down list, and the locked IP of the server will be displayed in the following list.
- Click Filter to add filtering conditions and the locked IPs which meet the conditions will be displayed in the following list.
- Click **Delete** in the Operation column, and the corresponded locked IP will be unlocked and deleted.
- Click the **Delete All** button above the list, and all the locked IPs in the list will be unlocked and deleted.

Notes:

- For how to configure the brute-force cracking defense, refer to AAA server.
- At most 2000 locked IPs can be displayed in the list. When the threshold is exceeded, the earliest locked IP will be unlocked and deleted in the list.

Authentication User

If system is configured with"Web Authentication" on Page 470, "Single Sign-On" on Page 485, "SSL VPN" on Page 605, "L2TP VPN" on Page 711the authentication user can gather statistics on the authenticated users. The column "IP/MAC" displays the IPv6 address of the authenticated users only when the system version is the IPv6 version.

Click **Monitor>Authenticated User**.



- Click Filter to select the condition in the drop-down list to filter the users. Filters include username/user group, AAA server, IP/IP range, and authentication type. You can set several filters at the same time.
- Click **Kick Out** under the Operation column to kick the user out.
- Click to refresh the real-time data in the list.

URL Hit

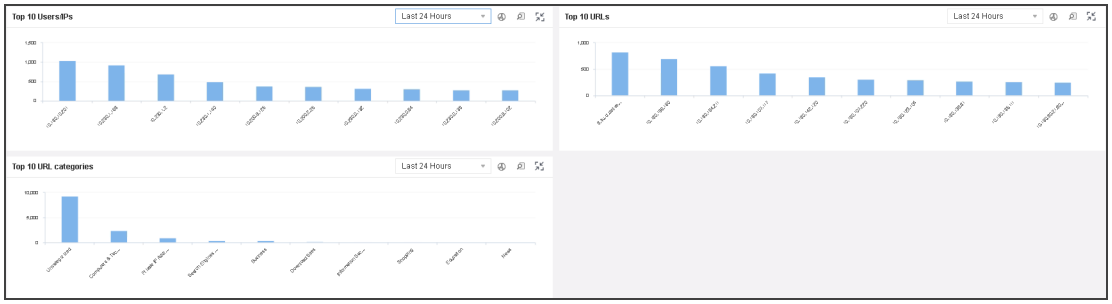
This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

If the " URL Filtering" on Page 992 function is enabled in the security policy rule, the predefined stat-set of URL filter can gather statistics on user/IPs, URLs and URL categories.

If IPv6 is enabled, system will support to monitor both IPv4 and IPv6 address.

Summary

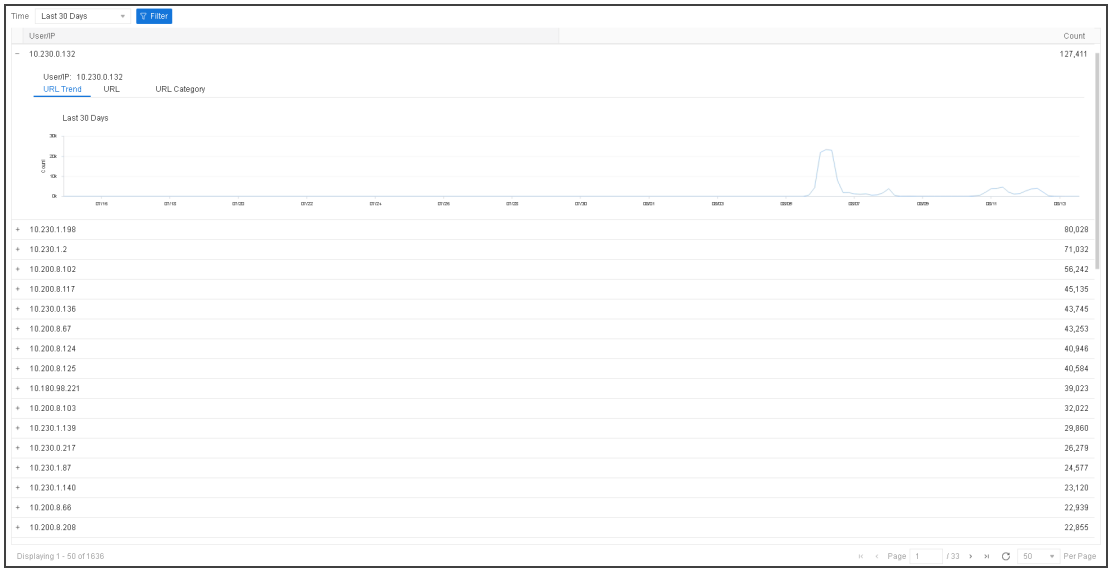
Click **Monitor> URL Hit>Summary**.



- Select a different Statistical_Period to view the statistical information in that period of time.
- Hover your mouse over a bar, to view the hit count of User/IP, URL or URL Category .
- Click at top-right corner of every table and enter the corresponding details.
- Click and to switch between the bar chart and the pie chart.

User/IP

Click **Monitor> URL Hit>User/IP**.



- The User/IPs and detailed hit count are displayed in the list below.
- Click a User/IP in the list to display the corresponding URL hit statistics in the curve chart below.
    - Statistics: Displays the hit statistics of the selected User/IP, including the real-time statistics and statistics for the latest 1 hour, 24 hours 30 days .
    - URL(real-time): Displays the URLs' real-time hit count of selected User/IP. Click URL link ,you can view the corresponding URLs detailed statistics page. Click **Detail** link, you can view the URL hit trend of the selected User/IP in the **URL Filter Details**dialog .
    - URL category(real-time): Displays the URL categories' read-time hit count of selected User/IP. Click URL category link , you can view the corresponding URL categories' detailed statistics page. Click **Detail** link, you can view the URL category hit trend of the selected User/IP in the pop-up dialog .
- Click the **Filter** button at top-left corner. Select **User/IP** and you can search the User/IP hit count information by entering the keyword of the username or IP.

URL

Click **Monitor > URL Hit > URL**.

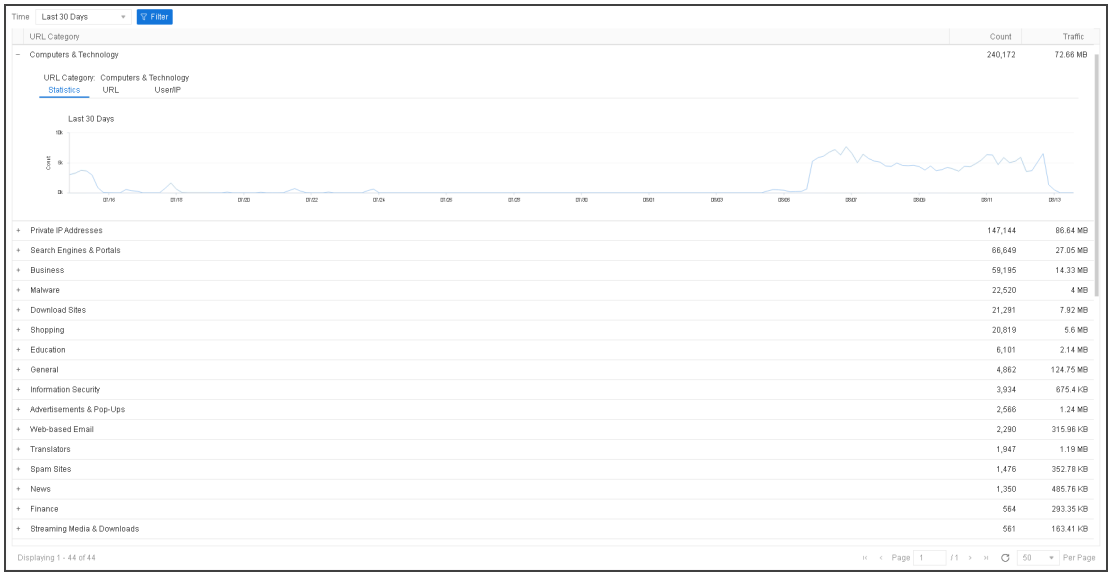
- The URL, URL category and detailed hit count are displayed in the list below.
- Click a URL in the list to view its detailed statistics.
    - Statistics: Displays the hit statistics of the selected URL, including the real-time statistics and statistics for the latest 1 hour, 24 hours 30 days .

- User/IP(real-time): Displays the User/IP's real-time hit count of selected URL. Click the User/IP link and you can view the corresponding user/IPs detailed statistics page. Click the **Detail** link and you can view the URL hit trend of the selected user/IP in the **URL Filter Details** page.

- Click the **Filter** button at the top-left corner. Select **URL**and you can search the URL hit count information by entering the keyword of the URL.
- Click to refresh the real-time data in the list.

URL Category

Click **Monitor> URL Hit > URL Category**.



- The URL category, count, traffic are displayed in the list.
- Click a URL category in the list to view its detailed statistics displayed in the Statistics, URL (real-time), User/IP(real-tiime) tabs.
    - Statistics: Displays the trend of the URL category visits, including the real-time trend and the trend in the last 60 minutes, 24 hours , 30 days.

- URL(real-time): Displays the visit information of the URLs, contained in the URL category, that are being visited.
- User/IP(real-time): Displays the visit information of the users or IPs that are visiting the URL category.

- Click  to refresh the real-time data in the list.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click the time button on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

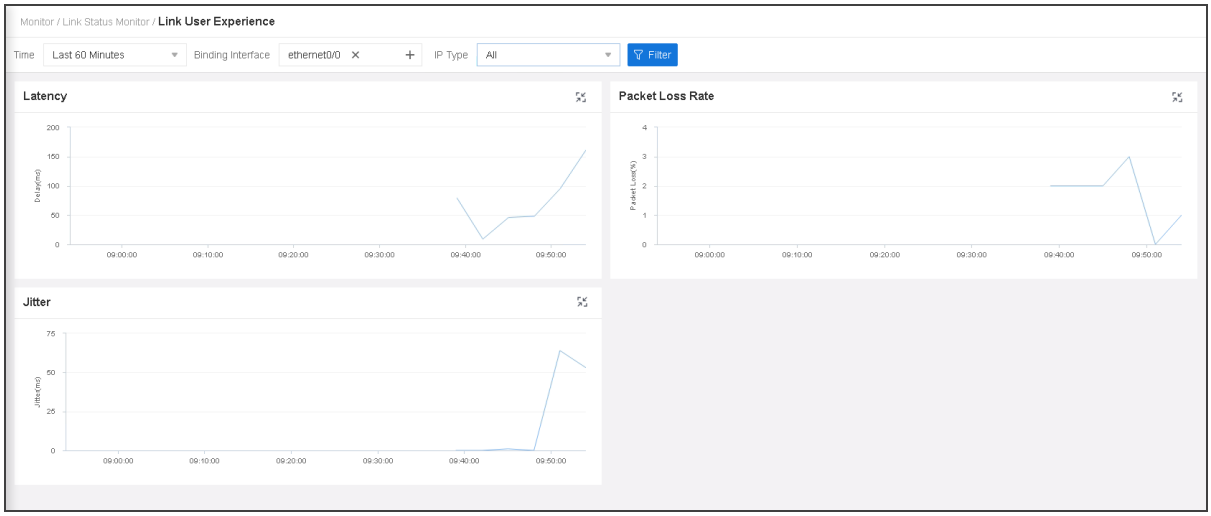
Link Status Monitor

Link status monitoring can calculate the sampling traffic information of the specific interface in the link, including latency, packet loss rate, and jitter, to monitor and display the overall status of the link. System also supports for link detection to calculate the traffic information of the specific destination IP address in the link, including latency, jitter, and packet loss rate, of the specific destination IP address or domain.

Link User Experience

The link user experience page displays the traffic statistics of the interfaces that have been bound within a specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month)

Click **Monitor > Link Status Monitor.** For more information about configuration of binding interfaces, refer to Link Configuration.



- Select a different Statistical_Period to view the statistical information in that periods of time.
- Select the binding interface **Binding Interface** drop-down list, Click the **Binding Interface** drop-down menu and select the interface name to view the link status monitoring statistics for this interface. You can select multiple interfaces.
- Click the **IP Type** drop-down menu and select the IP type to view the link status monitoring statistics for this IP type, including IPv4, IPv6 and All.
- Click Filter button and select **Application** in the drop-down menu. You can select the TOP 10 or Application / Application group name to view the link status monitoring statistics according to the specified application

Notes:

- "Time" , "Binding Interface" and "IP Type" are required in the filter condition, and "IP type" is selected as "All" by default.
- If the application switch of the specified interface is not enabled in the link configuration, the **Application** filter condition cannot be added.

Statistical Period

System supports the predefined time cycle and the custom time cycle. Click **Last 60 Minutes** on the top right corner of each tab to set the time cycle.

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

Link Detection

On the link detection page, you can configure a link detection rule to perform persistent link quality detection, and view persistent traffic statistics of specified detection destination IP/domain to link or link to detection destination IP/domain, including latency, jitter, and packet loss rate.

To configure the link detection, take the following steps:

1. Select **Monitor > Link Status Monitor > Link Detection**.
2. Click **New**.



Option	Description
Name	Specifies the name of the link detection rule.
Link	Select the interface whose link status you want to monitor from the drop-down list. You can select at most 8 interfaces. To create an interface whose link status you want to monitor, click **New**. At most 16 interfaces can be added. For more information, see Link Configuration.
Detection Destination	Select the detection destination IP address or domain whose link status you want to monitor from the drop-down list. You can select at most 8 detection IP addresses or 1 detection domain, but you cannot select detection IP address and domain at the same time. To create a detection destination whose link status you want to monitor, click **New**. At most 32 detection destinations can be added. For more information, see Detection Destination.
When packet loss rate is above	Specifies the packet loss rate threshold. When the packet loss rate exceeds the threshold, it is marked with a red dot in the packet loss trend chart. Valid values: 0% to 100%. Default value: 75%.
Description	Enter a description for the link detection rule.

3. Click **OK**. In the link detection list, you can view configured link detection. At most 24 link detection rules can be configured.

4. In the link detection list, select a link detection rule and click **Enable**. The system will pro-actively detect bidirectional traffic on the specified link to the specified destination. By

default, configured link detection rules are disabled.



5. Click in the **Operation** column to view the link detection quality, including traffic latency, jitter, and packet loss rate. The system allows you to view the latency, jitter, and packet loss rate of traffic within the last 3 minutes.



Notes:

- Non-root VSYS does not support the link detection function.
- The link detection function cannot be used in HA Active-Active mode.
- To delete a link detection rule, you can only disable the rule first and then delete it.
- All interfaces bound to a link detection rule need to belong to the same virtual router.
- When traffic latency is greater than or equal to 2000 ms, it is marked with a red dot in the latency trend chart.

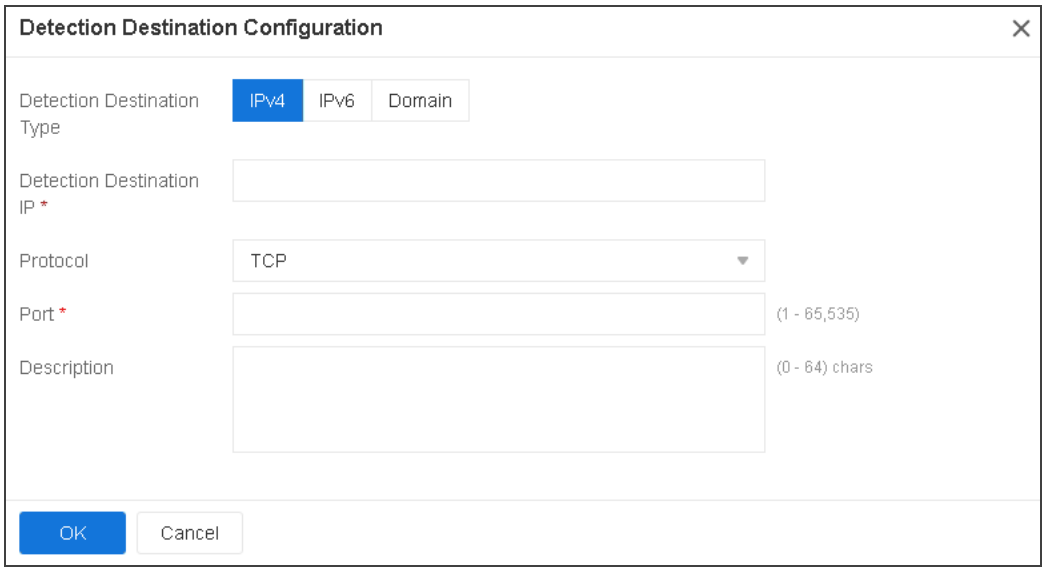
Detection Destination

On the detection destination page, you can configure the destination IP address to monitor the link state.

To configure the detection destination, take the following steps:

1. Select **Monitor > Link Status Monitor > Link Detection**. On the **Link Detection** page, click **Detection Destination** in the upper-right corner.

2. Click **New**.



Option	Description
Detection Destination Type	Specifies the address type of the detection destination. Valid values: IPv4, IPv6, and Domain.
Detection Destination IP	Specifies the IP address of the detection destination. This parameter is required only if you set the detection destination type to **IPv4** or **IPv6**.
Domain Detect Type	Specifies the detection type of the domain. This parameter is required when you set the detection destination type to **Domain**. Valid values: IPv4 and IPv6.
Domain	Specifies the domain of the detection destination. This parameter is required only if you set the detection destination type to **Domain**.
Protocol	Specifies the protocol type of the detection destination. Valid

Option	Description
	values: TCP and ICMP.
Port	Specifies the port number of the detection destination. Valid values: 1 to 65535. This parameter is required only if you set the protocol type to **TCP**.
Description	Enter a description for the detection destination.

3. Click **OK**.

Link Configuration

In the link configuration page, you can configure the binding interface to monitor the link state and can enable the application switch and link user experience.

To configure the link, take the following steps:

1. Click **Monitor > Link Status Monitor > Link Configuration**.
2. Click **New**.



Option	Description
Binding Inter-	Select the interface in the drop down menu.

Option	Description
face	
Interface Description	Type the description for the interface.
Application	Click the **Enable** button. After enabling, you can see details of the specific application in this interface.
Monitor	Click the **Enable** button. After enabling, you can see traffic statistics in this interface.

3. Click **OK**.

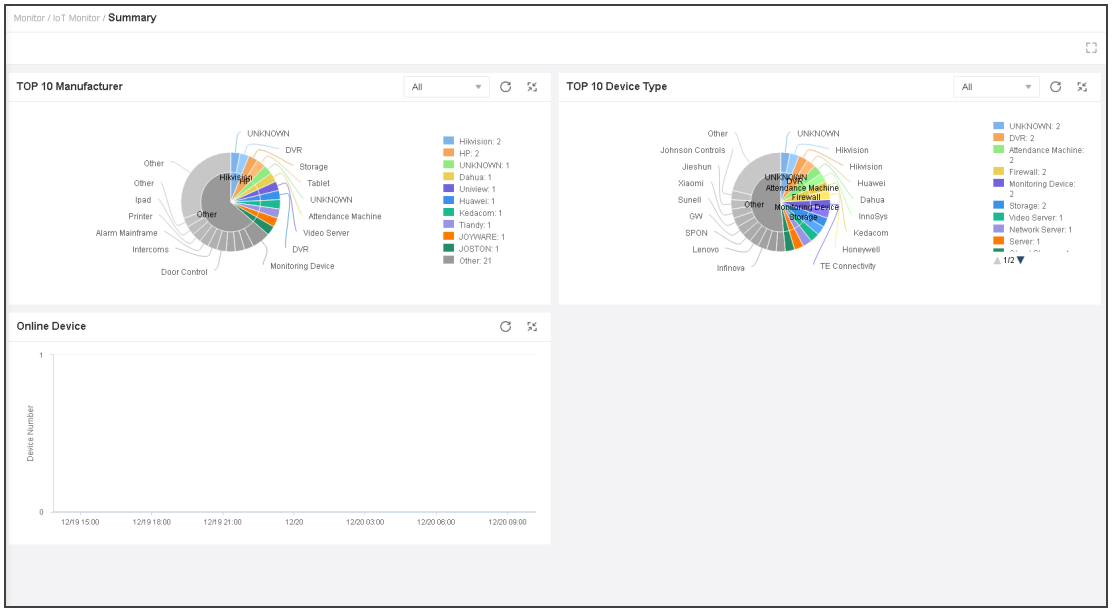
IoT Monitor

IoT Monitor function displays the manufacturers and types distribution of network video monitoring devices, as well as the detailed statistics, such as device number, IP address, MAC address, up/downstream traffic, IoT profile and device status.

Summary

On the Summary page, you can obtain the real-time distribution of manufacturers and device types.

Click **Monitor** > **IoT Monitor** > **Summary**.

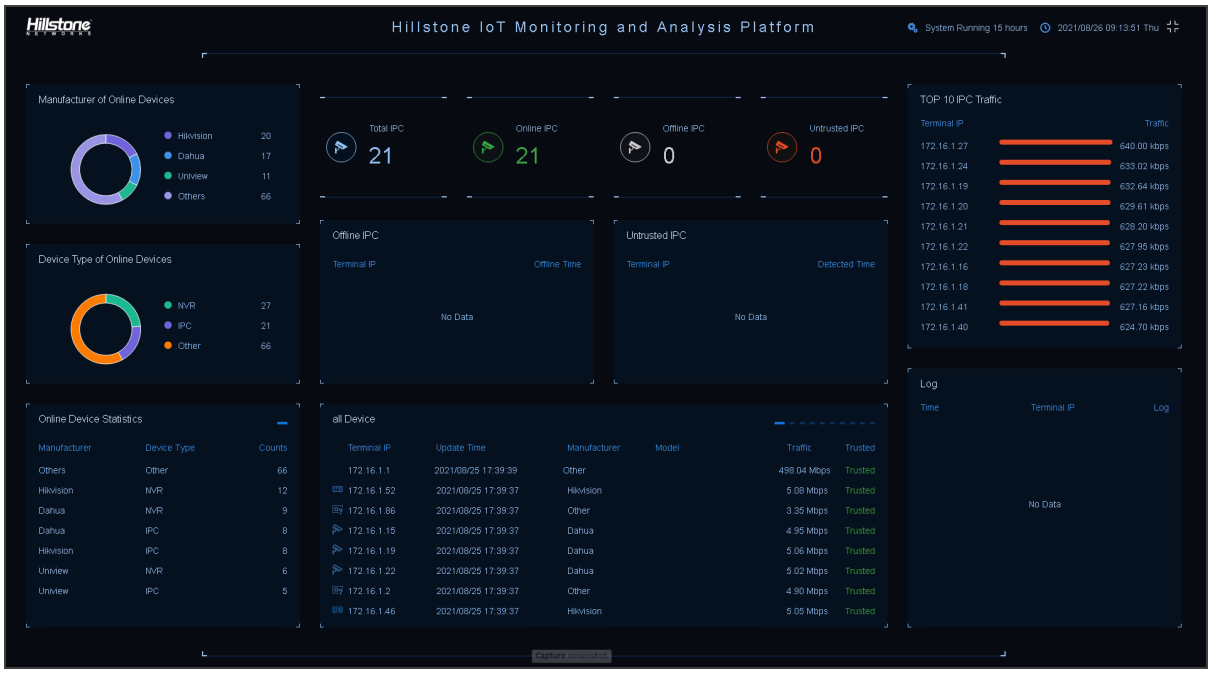


- Select Online/Offline/All from the drop-down list in the upper-right corner to view manufacturers and device types in the corresponding status.
- Click the button to refresh the monitoring data.
- Hover your mouse over the bar chart to view the device number of different manufacturers and different device types.
- Hover your mouse over the line chart to view the number of online devices.
- Different manufactures and devices are marked with different colors of legends. When your mouse hovers over an legend, the corresponded part will be highlighted on the bar chart.
- Click the button to enter the screening monitoring mode.

Screening Monitoring Mode

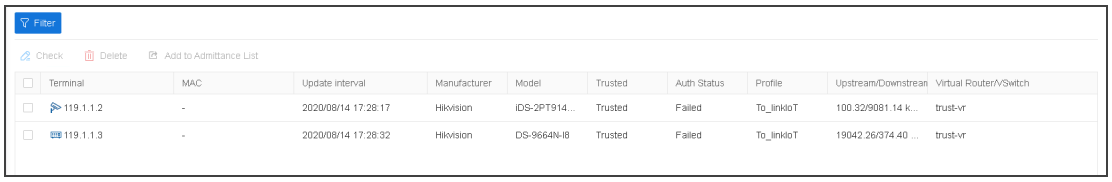
The screening monitoring mode of IoT monitor displays various statistical information such as the manufacturer, type, number of cameras, and traffic of online network video monitoring device in a more intuitive way.

Click the button in the upper right corner of the summary page to enter the screening monitoring mode.



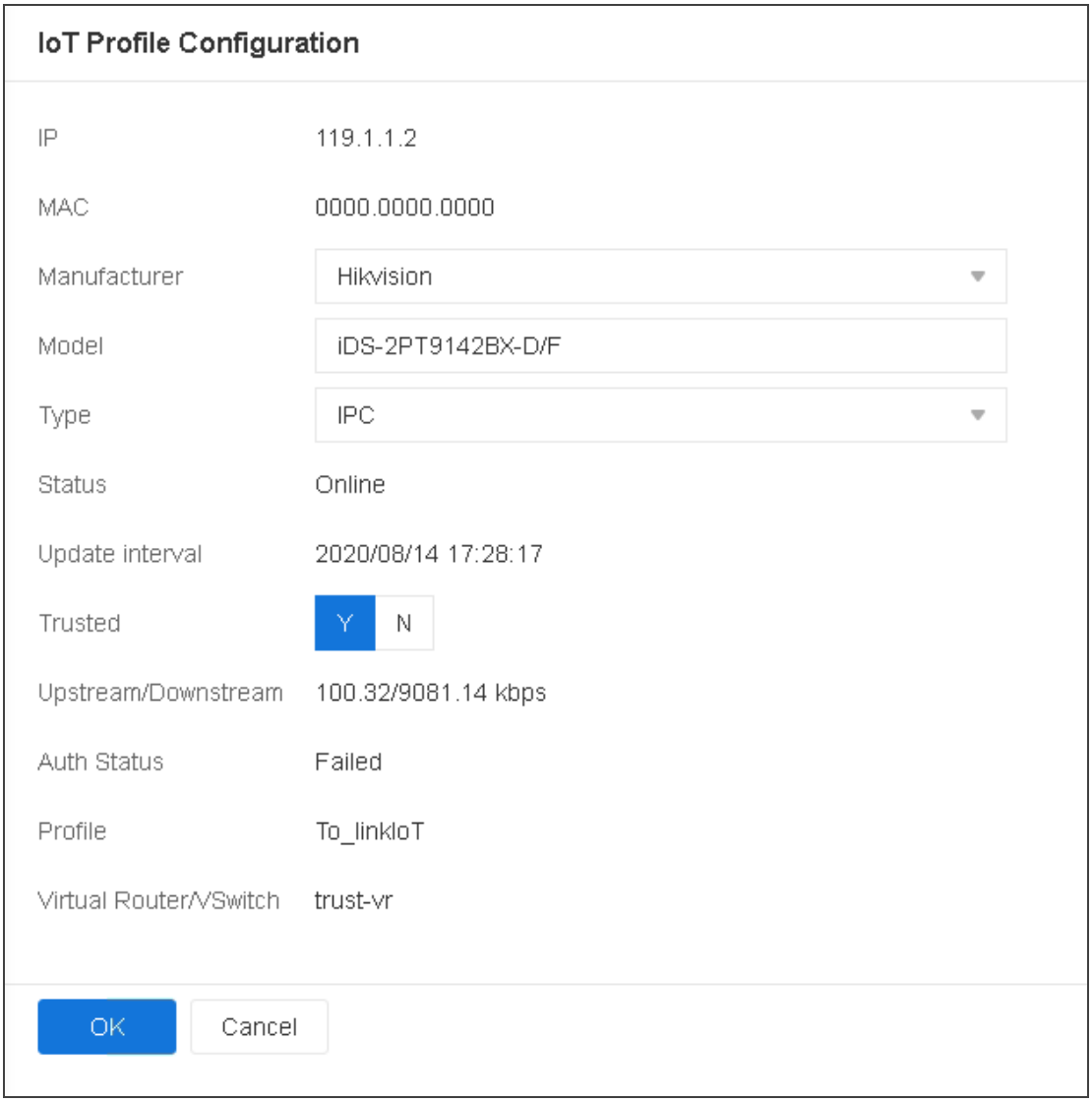
Details

Click **Monitor** > **IoT Monitor** > **Details** to view the detailed information of the network video monitoring devices.



- Click the Filter button to add filter conditions and the required information will be filtered out in the following list.
- Select the check box, and click **Delete** to delete the selected item.

- Select the check box, and click **Check**, then the **IoT Profile Configuration** page pops up. You can modify the manufacturer, model, type and trust status manually. The manually changed configuration is prior to the automatically detected result. When the device logs in again, the manually changed configurations will be cleared.



- Select the check box and click **Add to Admittance List** to add the selected item to the target admittance list template. For the detailed steps, refer to Adding to Admittance List.
- Click **Add to Respository** to add the selected network video monitor device to the repository.

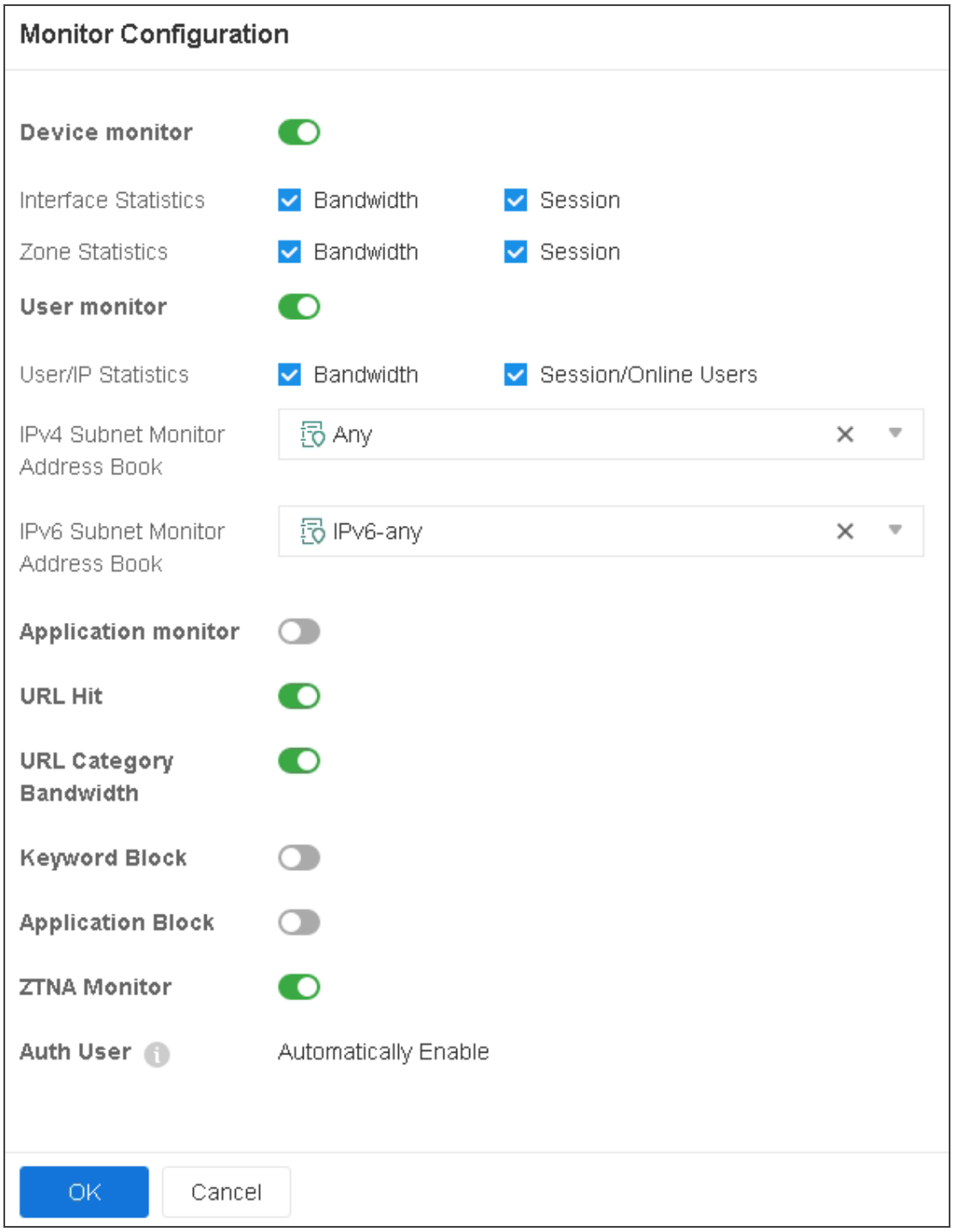
- Click **Remove From Respository** to remove the selected network video monitor device from the repository.
- For the icons in the **Terminal** list, if the icon is gray, it means that the device is offline; if the icon is blue, it means that the device is online. When you hover the mouse over the icon, you can also view the online status of the device. The icons represent the following devices respectively:
  - : The network video monitoring devices of other manufacturers.
  - : The IPC device.
  - : The NVR device.
  - Null: The item hasn't been identified.

Monitor Configuration

You can enable or disable some monitor items as needed. The monitor items for Auth user are enabled automatically.

To enable/disable a monitor item, take the following steps:

1. Click **Monitor > Monitor Configuration**.



2. Select or clear the monitor item(s) you want to enable or disable.

3. Select subnet monitor address book in the IPv4 Subnet Monitor Address Book or IPv6 Subnet Monitor Address Book drop-down list. The system will match the traffic which is sent from the Internet to Subnet according to the specified address. If matched, the traffic will be counted to the Subnet side. You can click ▼ in the search box and enter the name and member IP address of an address book for a fuzzy search. The name and member IP address are in the logical AND relation.
4. Click **OK**.



Notes:

- In the **Address** field, you can enter a variety of address sources. For example, if you enter "10.10.10.10/32", an address book that contains the address member 10.10.10.10/24 may be matched; if you enter "9.9.9.9/24", an address book that contains the address member 9.9.0.0/16 may be matched; if you enter "10.10.10.10", an address book that contains the addresses member whose IP range is 10.10.10.0-10.10.10.255 may be matched; if you enter "10.23", an address book that contains the address member 1.10.23.10/24 may be matched; if you enter "aa", an address book that contains the address member whose hostname is aaa may be matched.
- After a monitor item is enabled or disabled in the root VSYS, the item of all VSYSs will be enabled or disabled(except that the non-root VSYS does not support this monitor item). You can not enable or disable monitor item in non-root VSYSs.

Long-term Monitor

The system supports the long-term monitor function. This function can be used to continuously monitor and collect statistics on device traffic and sessions and then store these statistics, which

meets your requirements for network monitoring and diagnostics. The detailed function is described as follows.

- Supports the storage of statistics for device traffic and sessions over the last 180 days to the device disks. You are allowed to set limits on the size of the statistics storage space.
- Supports query by IP or application type. You can query data from a maximum of 31 consecutive days within the last 180 days.
- Supports the display of statistics in lists, bar charts, and line charts.

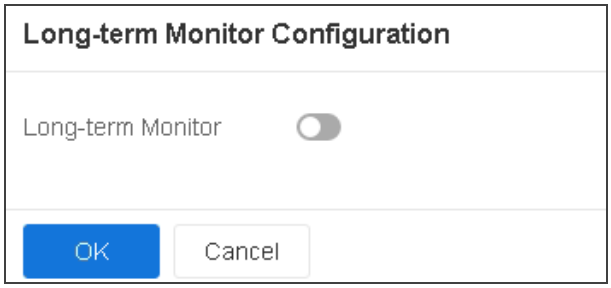
Notes: The long-term monitor function is available only for:

- SG-6000 A-Series devices installed with hard disks(excluding SG-6000-A1605/A1805/A2205).

Long-term Monitor Configuration

By default, the Long-term Monitor function is disabled. To enable this function, take the following steps:

1. Select **Monitor** > **Long-term Monitor** > **Configuration**.



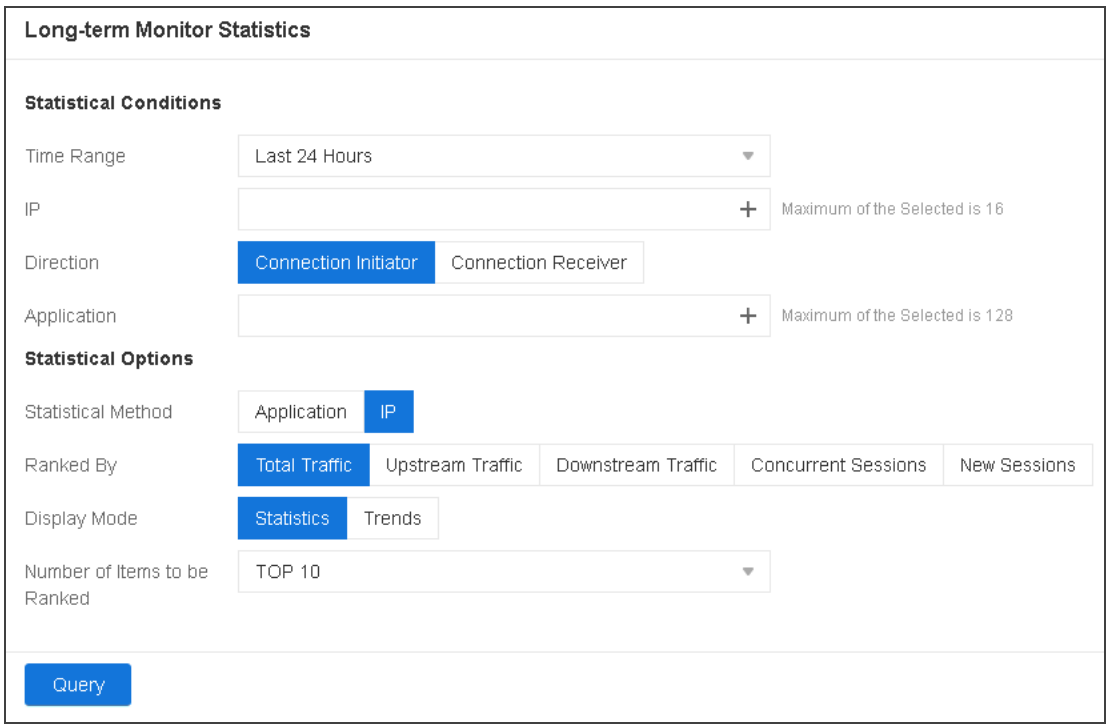
2. On the **Long-term Monitor Configuration** page, enable **Long-term Monitor**.
3. Click OK.

Long-term Monitor Statistics

You can specify query conditions for long-term monitor statistics.

To specify query conditions and view corresponding statistics, take the following steps:

1. Select **Monitor** > **Long-term Monitor** > **Query**.

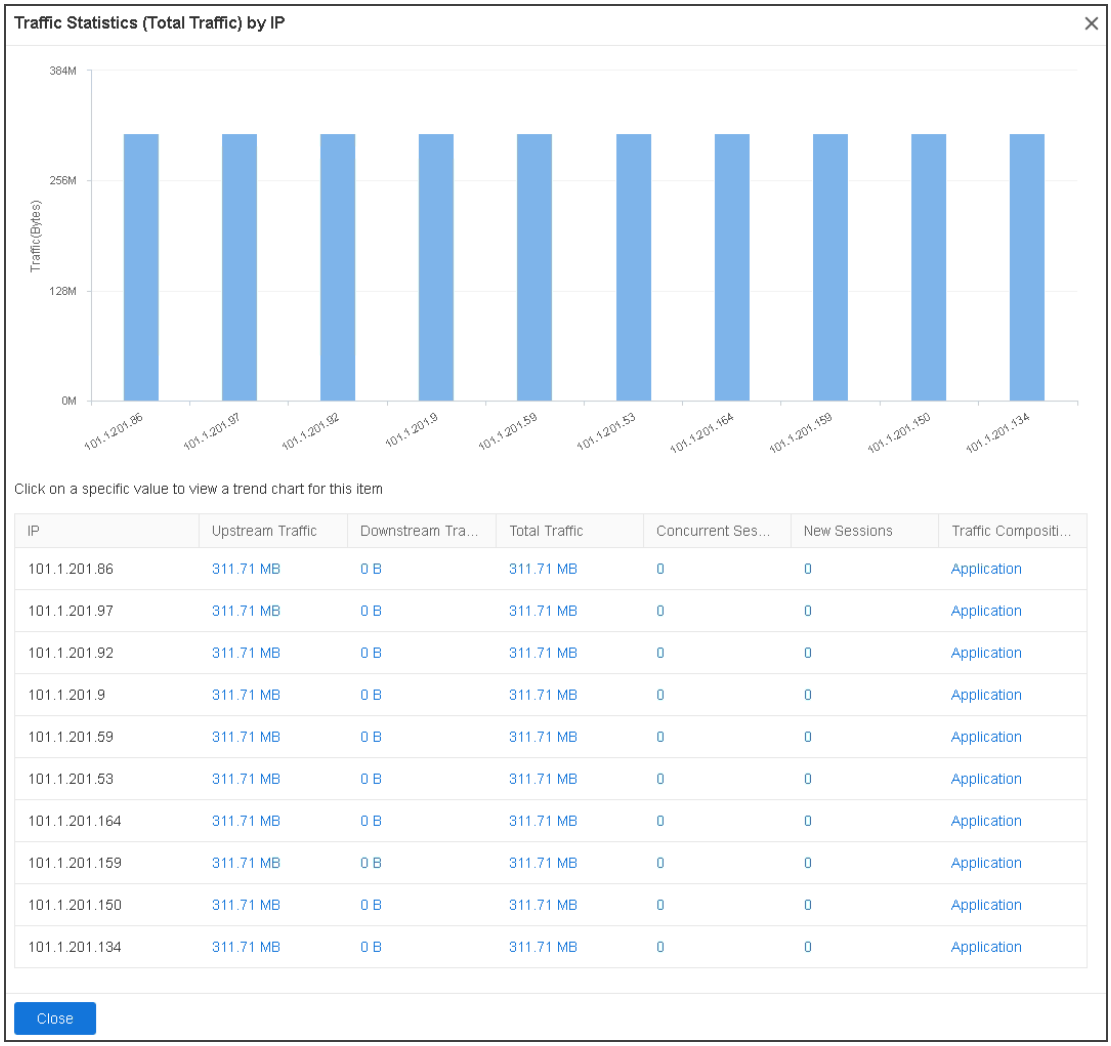


Option	Description
Statistical Conditions	
Time Range	Select a time range from the drop-down list to view statistics within the specified time range: • Last 60 Minutes: displays the statistics of the last 60 minutes. • Last 24 Hours: displays the statistics of the last 24 hours.

Option	Description
	• Last 7 Days: displays the statistics of the last 7 days. • Last 30 Days: displays the statistics of the last 30 days. • Custom: Customize the statistical period. After you select this option, specify the start time and end time in the **Custom Date and Time** panel. You can specify a statistical period of at most 31 consecutive days within the last 180 days。
IP	Specifies the IP address whose traffic statistics you want to collect, which can be IP/Netmask, IPv4 Range, IPv6/Prefix, or IPv6 Range. To add an IP entry, click “+”, select an IP type, enter the corresponding values in the field below, and then click **Add**. Multiple IP entries can be added.
Direction	Specifies the direction of traffic statistics to be collected. Valid values: Connection Initiator and Connection Receiver.
Application	Specifies the application whose traffic statistics you want to collect, which can be a predefined or custom application. To add an application, click “+” and select an application. Multiple applications can be added. You can also click “+” to create an application. For more information, see Creating a User-defined Application.
Statistical Options	
Statistical Method	Specifies the method based on which statistical data is displayed.

Option	Description
Ranked By	Specifies the type of traffic size based on which statistical data is ranked.
Display Mode	Specifies the mode based on which statistical data is displayed.
Number of Items to be Ranked	Specifies the number of items whose traffic statistics you want to collect. If the Display Mode parameter is set to Statistics, traffic statistics of the top 10, top 20, and top 50 items can be collected and displayed. If the Display Mode is set to Trends, traffic trends of only the top 10 items can be collected and displayed.

2. Click **Query**. In the panel that appears, the statistical data is displayed (The following figure shows the traffic statistics by IP address):



- Hover your mouse over the column chart to view the number of concurrent sessions of the IP address.
- Find an IP address and click the value in the **Upstream Traffic** column to view the trend chart of the upstream traffic of the IP address.
- Find an IP address and click the value in the **Downstream Traffic** column to view the trend chart of the downstream traffic of the IP address.

- Find an IP address and click the value in the **Total Traffic** column to view the trend chart of the total traffic of the IP address.
- Find an IP address and click the value in the **Concurrent Sessions** column to view the trend chart of the concurrent sessions of the IP address.
- Find an IP address and click the value in the **New Sessions** column to view the trend chart of the new sessions of the IP address.
- Find an IP address and click Application in the **Traffic Composition** column to view the applications from which the traffic of the IP address comes.

Long-term Monitor Storage Size Settings

The system allows you to store long-term monitor statistics of device traffic and sessions to the device disks. A default amount of storage size is allocated to long-term monitor statistics. You can customize the storage size as required. For more information, see Storage Manage, see Storage Management.

Logging

Logging is a feature that records various kinds of system logs, including device log, threat log, session log, NAT log, Content filter log, File filter log, share access logs, and URL logs.

- Device log
  - Event - includes 8 severity levels: debugging, information, notification, warning, error, critical, alert, emergency.
  - Network - logs about network services, like PPPoE and DDNS.
  - Configuration - logs about configuration on command line interface, e.g. interface IP address setting.

- Threat - logs related to behaviors threatening the protected system, e.g. attack defense and application security.
- Session - Session logs, e.g. session protocols, source and destination IP addresses and ports.
- NAT - NAT logs, including NAT type, source and destination IP addresses and ports.
- EPP - logs related with end point protection function.
- File Filter - logs related with file filter function.
- Content filter logs – logs related with content filter function, e.g. Web content filter, Web posting, Email filter and HTTP/FTP control.
- Network behavior record logs – Logs related with network behavior record function, e.g. IM behavior ,etc.
- URL - logs about network surfing, e.g. Internet visiting time, web pages visiting history, an URL filtering logs.
- PBR - logs about policy-based route.
- CloudSandBox - logs about sandbox.
- Share Access Logs - logs about share access rule.

The system logs the running status of the device, thus providing information for analysis and evidence.

Log Severity

Event logs are categorized into eight severity levels.

Severity	Level	Description	Log Definition
Emergencies	0	Identifies illegitimate system events.	LOG_ EMERG

Severity	Level	Description	Log Definition
Alerts	1	Identifies problems which need immediate attention such as device is being attacked.	LOG_ALERT
Critical	2	Identifies urgent problems, such as hardware failure.	LOG_CRIT
Errors	3	Generates messages for system errors.	LOG_ERR
Warnings	4	Generates messages for warning.	LOG_WARNING
Notifications	5	Generates messages for notice and special attention.	LOG_NOTICE
Informational	6	Generates informational messages.	LOG_INFO
Debugging	7	Generates all debugging messages, including daily operation messages.	LOG_DEBUG

Destination of Exported Logs

Log messages can be sent to the following destinations:

- Console - The default output destination. You can close this destination via CLI.
- Remote - Includes Telnet and SSH.
- Buffer - Memory buffer.
- File - By default, the logs are sent to the specified USB destination in form of a file.
- Syslog Server - Sends logs to UNIX or Windows Syslog Server.

- Email - Sends logs to a specified email account.
- Local database - Sends logs to the local database of the device.

Log Format

To facilitate the access and analysis of the system logs, StoneOS logs follow a fixed pattern of information layout, i.e. **date/time, severity level@module: descriptions**.See the example below:

2000-02-05 01:51:21, WARNING@LOGIN: Admin user "admin" logged in through console from localhost.

Event Log

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view event logs, select **Monitor > Log > Event Log**.

In this page, you can perform the following actions:

- Filter: Click Filter to add conditions to show logs that march your filter.
- Configure: Click to jump to the configuration page.
- Export: Click to export the displayed logs as a TXT or CSV file.Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.

Network Log

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view network logs, select **Monitor > Log > Network Log**.

In this page, you can perform the following actions:

- Filter: Click 

to add conditions to show logs that march your filter.
- Configure: Click to jump to the configuration page.
- Export: Click to export the displayed logs as a TXT or CSV file.Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.

Configuration Log

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view configuration logs, select **Monitor > Log > Configuration Log**.

In this page, you can perform the following actions:

- Filter: Click 

to add conditions to show logs that march your filter.
- Configuration: Click to jump to the configuration page.
- Export: Click to export the displayed logs as a TXT or CSV file.Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.

Share Access Logs

To view share access logs, select **Monitor > Log > Share Access Log**.

In this page, you can perform the following actions:

- Configuration: Click to jump to the Log Management page.
- Export: Click to export the displayed logs as a TXT or CSV file.

- Add to My Log: Click to add the current filtered results to MyLog list.
- Filter: Click  to add conditions to show logs that march your filter.

Threat Log

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

Threat logs can be generated under the conditions that:

- Threat logging in the Logging feature is enabled. Refer to "Managing Logs" on Page 1587.
- You have enabled one or more of the following features: , " Intrusion Prevention System" on Page 1315, "Attack-Defense" on Page 1389 or "Perimeter Traffic Filtering" on Page 1279 .

To view threat logs, select **Monitor > Log > Threat Log**.

In this page, you can perform the following actions:

- Click  to configure more filter conditions. After configure the filter conditions, the system will automatically display the matched logs. For devices that are of the IPv6 version, the filter conditions for source and destination addresses support both IPv4 and IPv6. Click the drop-dow menu after the **Filter** and select "Save Filter" to save the current filter conditions, so that the next time you can directly select the save filter conditions, and view the corresponding log. When selecting **Attack Result**, view the threat log of the specified attack result, including:
  - Attempted: Indicates that an attack occurs, but the attack is unsuccessful or the result of the attack is uncertain, and it is impossible to determine whether the attacked device has compromised.
  - Successful: The attacker has successfully exploited the vulnerability or delivered a malicious sample, and it is unclear whether the malicious sample is executed.

    - Confirmed Compromised: It is confirmed that the attacked device has been compromised, and there have been behaviors such as outreach and lateral spread.
    - Unknown: Upgrading the attack results from the old database or the attack results preset by the unsupported detection engine.
- Merge Log: Select the merge type from the drop-down list, which includes Do Not Merge, Threat Name, Source IP, Destination IP.
- Configure: Click to jump to the configuration page.
- Export: Click to export the displayed logs as a TXT or CSV file.Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.
- Click a threat log name in the table and then you can view the detailed information in the Log Details tab. In the Log Details tab, you can do the following:
    - View the severity, application/protocol, source/destination port, threat start time, end time, and other threat-related information (such as plain-text SQL command, plain-text paths to URI, etc.).
    - Click "ViewPcap" to see the message package of the threat, or click "Download" to download the packet to local for viewing. IPv6 and IPv4 protocol type messages are both supported for users to view.
    - For threat logs related to weak password, click **View** behind the **Password** field. The administrator can view weak password details in the **Password View** panel. Click **Copy** to copy the weak password.
    - Click "Signature ID" "Add Whitelist" "Disable Rule" to quickly link to the relevant page.

- When the detection engine is anti-virus, click the name of the log entry whose details you want to view in the log list. You can click **Add to Whitelist** next to MD5 or URL to add this MD5 or URL to the whitelist list in **Object** > **Anti-Virus** > **Whitelist**.
- For threat logs whose detection engine is IPS, if you enable the **Capture Threat Data** function, you can view ASCII and hex information of the threat in the Log Details tab. With the help of data in the **Threat Data** section, you can analyze the whole development process of the threat. If the **Capture Threat Data** function is not enabled, the **Threat Data** option will not be displayed on the **Threat Log** page. This function can be enabled only by using the CLI. For more information, visit **Threat_Prevention** > **IPS_config** in *StoneOS CLI User Guide*.
- For threat logs whose detection engine is IPS or antivirus, you can click **Add Blacklist** behind the attacker to block the IP address of the attack source by adding it into the blacklist. For more information about how to configure IP blacklist, refer to Static IP Blacklist.
- MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) is a knowledge base of attack behaviors. It categories known attacks as tactics and techniques, establishing a practical and clear framework. The system maps detected suspicious behaviors to the MITRE ATT&CK® model and displays the MITRE ATT&CK® tactic IDs and MITRE ATT&CK® technique IDs of the threat in threat logs, helping you identify suspicious behaviors in a better way. To ensure that the latest MITRE ATT&CK® knowledge base is used during detection, it is recommended to upgrade the MITRE ATT&CK® knowledge database. For more information about upgrading the MITRE ATT&CK®Knowledge Base, refer to Updating Signature Database.

- Click **MITRE ATT&CK® Tactic ID** to go to the **MITRE ATT&CK® Tactic Details** panel, where you can view the name, created time, last modified time, data source, official link, and description of this tactic. MITRE ATT&CK® Tactic represents the tactical object of adversary and the reason for performing the attack.
- Click **MITRE ATT&CK® Technical ID** to go to the **MITRE ATT&CK® Technical Details** panel, where you can view this technique's name, data source, permission/system/network requirements, tactic, parent technique, sub technique, mitigation methods, official link, platform, ect. MITRE ATT&CK® Technique represents how an adversary achieves a tactical goal by performing an action.

- The system supports to upload certain elements (such as IP address) in logs generated from each module to the cloud platform. The cloud platform will query whether the element carries threat intelligence by using the third-party server. You can view details about threat intelligence of the element via CloudVista.
  - In the threat list, click the threat intelligence icon (, , or ) behind the address in the "Source"/"Destination" column in the list, or hover your cursor over a object, and there is a button () to its right. Click this button to open the threat intelligence center (CloudVista) to view the threat intelligence.
  - Threat intelligence status:  indicates a normal intelligence that contains the whitelist;  indicates a suspicious intelligence;  indicates a malicious intelligence.



Notes:

- The threat intelligence function is controlled by license. Before you use the function, you need to install the corresponding license.

- Before you use the function, configure "Connecting to Hillstone Cloud Service Platform" on Page 1770.

Session Log

Session logs can be generated under the conditions that:

- Session logging in the Logging feature is enabled. Refer to "Managing Logs" on Page 1587.
- The logging function has been enabled for policy rules. Refer to "Security Policy" on Page 1089.

To view session logs, select **Monitor > Log > Session log**.



- Click Filter to specify filter conditions. The session logs that meet the filter conditions are displayed in the list.
  - Time - Displays session logs within the specified time range (last 60 minutes, last 24 hours, last 7 days, last 30 days, and custom). By default, last 24 hours is selected.

- Policy ID - Displays session logs of policy rule of the specified ID.
- Source IP - Displays session logs of the specified source IP address.
- AAA: user@host - Displays session logs of user of the specified AAA server.
- Source Port - Displays session logs of the specified source port.
- Destination IP - Displays session logs of the specified destination IP address.
- Destination Port - Displays session logs of the specified destination port.
- Protocol - Displays session logs of the specified protocol.
- Action - Displays session logs of the specified action.
- Application - Displays session logs of the specified application.
- Source Interface - Displays session logs of the specified source interface.
- Destination Interface - Displays session logs of the specified destination interface.
- Close Reason - Displays session logs of the specified termination reason.

- Configure: Click this button to configure session logs.
- Clear: Click this button to clear all session logs stored in the system. (Note: The **Clear** option is not supported for devices that support sending log information to the local database.)
- Export: Export all session logs stored in the system or filtered results (filter first, and then export) as a TXT or CSV file. You can add an encryption password to the exported file so that the users need to enter the password to view the file.
- Specify the number of session logs to be displayed: Select a number from the **Data Limit** drop-down list to specify the number of session logs that meet the filter conditions. Valid values: 1000, 10000, 50000, and 100000. Default value: 1000.

Notes:

- For ICMP session logs, the system will only record the ICMP type value and its code value. As ICMP 3, 4, 5, 11 and 12 are generated by other communications, not a complete ICMP session, system will not record such kind of packets.
- For TCP and UDP session logs, system will check the packet length first. If the packet length is 20 bytes (i.e., with IP header, but no loads), it will be defined as a malformed packet and be dropped; if a packet is over 20 bytes, but it has errors, system will drop it either. So, such abnormal TCP and UDP packets will not be recorded.

PBR Log

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

PBR logs can be generated under the conditions that:

- PBR logging in the Logging feature is enabled. Refer to "Managing Logs" on Page 1587.
- You have enabled logging function in PBR rules. Refer to "Creating a Policy-based Route Rule" on Page 380 .

To view PBR logs, select **Monitor > Log > PBR Log**.

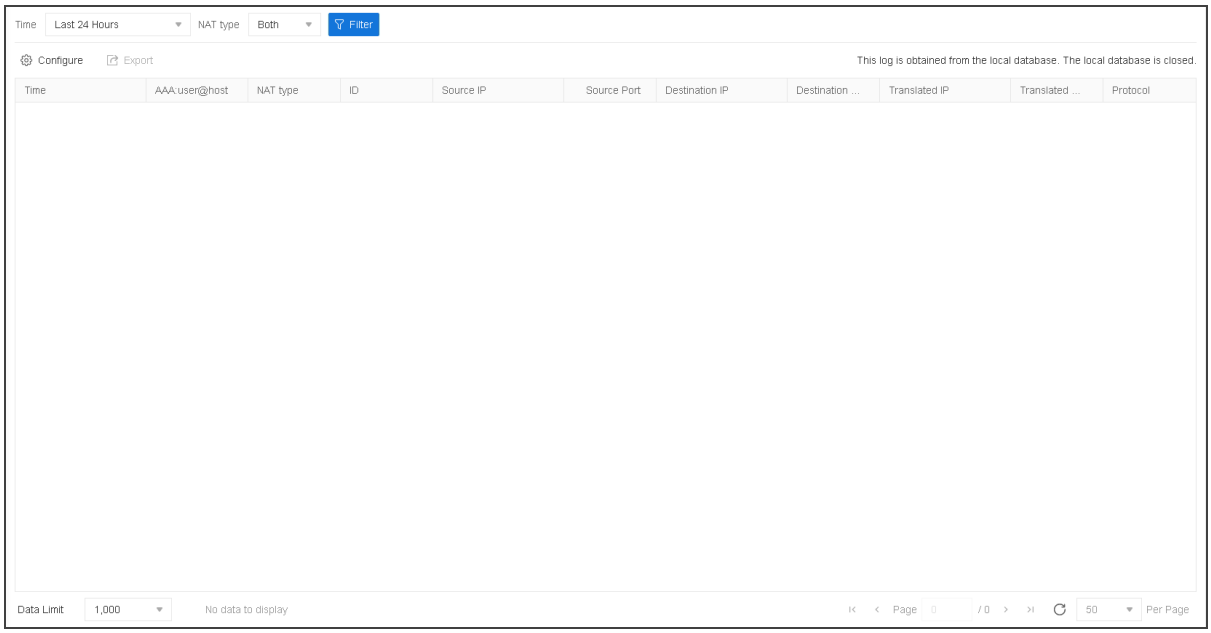


NAT Log

NAT logs are generated under the conditions that:

- NAT logging in the Logging feature is enabled. Refer to "Managing Logs" on Page 1587.
- NAT logging of the NAT rule configuration is enabled. Refer to"Configuring SNAT" on Page 1182 and"Configuring DNAT" on Page 1200.

To view NAT logs, select **Monitor > Log > NAT Log**.



- Click Filter to specify filter conditions. The NAT logs that meet the filter conditions are displayed in the list.
- Configure: Click this button to configure NAT logs.
- Clear: Click this button to clear all NAT logs stored in the system. (Note: The **Clear** option is not supported for devices that support sending log information to the local database.)
- Export: Export all NAT logs stored in the system or filtered results (filter first, and then export). You can add an encryption password to the exported file so that the users need to enter the password to view the file.

- Specify the number of NAT logs to be displayed: Select a number from the **Data Limit** drop-down list to specify the number of NAT logs that meet the filter conditions. Valid values: 1000, 10000, 50000, and 100000. Default value: 1000.

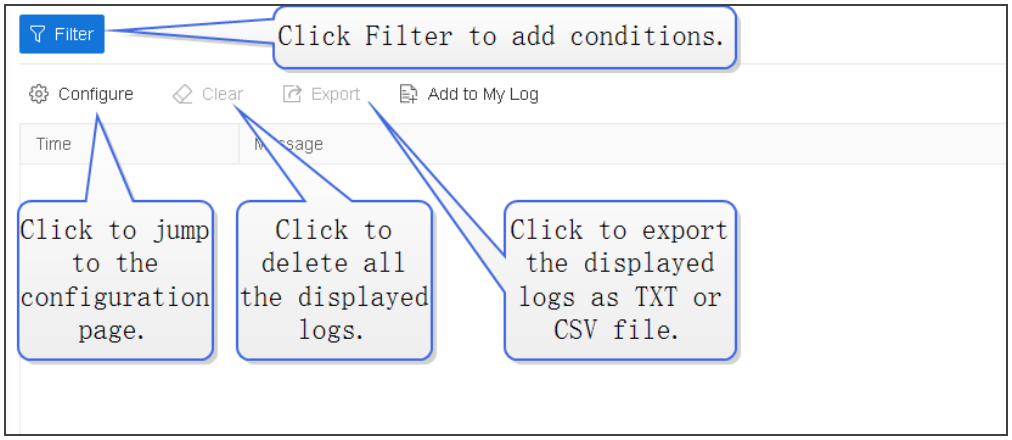
URL Log

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

URL logs can be generated under the conditions that:

- URL logging in the Logging feature is enabled. Refer to "Managing Logs" on Page 1587.
- You have enabled logging function in URL rules. Refer to " URL Filtering" on Page 992

To view URL logs, select **Monitor > Log > URL Log**.



EPP Log

To view EPP logs, select **Monitor > Log > EPP**.

In this page, you can perform the following actions:

- Configuration: Click to jump to the EPP page.
- Clear: Click to clear the selected logs.

- Export: Click to export the displayed logs as a TXT or CSV file.Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.
- Filter: Click 

to add conditions to show logs that march your filter.

IoT Log

You can view, configure, clear or export IoT logs.

The following condition should be met before log's generation:

- The IoT logging function has been enabled on the device. For the detailed configurations, refer to Log Management.

Click **Monitor** > **Log** > **IoT Log** to enter the <IoT Log> page.

- Click the 

button to add filter conditions and the required information will be filtered out in the following list.
- Configure: Click the **Configure** button and enter the **Log Management** page.
- Clear: Click the **Clear** button to delete all the filtered IoT logs in system.
- Export: Click the **Export** button to export part or all logs in the format of TXT or CSV. Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.

File Filter Log

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

File Filter logs can be generated under the conditions that:

- File Filter logging in the Logging feature is enabled. Refer to "Managing Logs" on Page 1587.
- You have enabled the function of "File Filter" on Page 1033.

To view File Filter logs, select **Monitor > Log > File Filter**.

- Filter: Click Filter to add conditions to show logs that march your filter
- Configure: Click to jump to the configuration page
- Clear: Click to delete all the displayed logs.
- Export: Click to export the displayed logs as a TXT or CSV file. Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.

Content Filter Log

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Content Filter logs can be generated under the conditions that:

- Content Filter logging in the Logging feature is enabled. Refer to "Managing Logs" on Page 1587.
- You have enabled one or more of the following features: "Web Content" on Page 1042, "Web Posting" on Page 1048, "Email Filter" on Page 1054 and"APP Behavior Control" on Page 1059 function.

To view Content Filter logs, select **Monitor > Log > Content Filter**.

- Filter: Click Filter to add conditions to show logs that march your filter
- Configure: Click to jump to the configuration page
- Clear: Click to delete all the displayed logs.

- Export: Click to export the displayed logs as a TXT or CSV file. Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.

Network Behavior Record Log

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

Network Behavior Record logs can be generated under the conditions that:

- Network Behavior Record logging in the Logging feature is enabled. Refer to "Managing Logs" on Page 1587.
- You have enabled the function of"Network Behavior Record" on Page 1066.

To view Network Behavior Record logs, select **Monitor > Log > Network Behavior Record**.

- Filter: Click Filter to add conditions to show logs that march your filter
- Configure: Click to jump to the configuration page
- Clear: Click to delete all the displayed logs.
- Export: Click to export the displayed logs as a TXT or CSV file. Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.

CloudSandBox Log

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view sandbox logs, select **Monitor > Log > Cloud SandBox Log**.

In this page, you can perform the following actions:

- Configure: Click to jump to the CloudSandBox page.
- Clear: Click to clear the selected logs. (Note: This option is not supported for devices that support sending log information to the local database)
- Export: Click to export the displayed logs as a TXT or CSV file.Then, you can add an encryption password to the exported file based on your requirements. This way, only users that enter the specified password can view this file.
- Filter: Click 

to add conditions to show logs that march your filter.

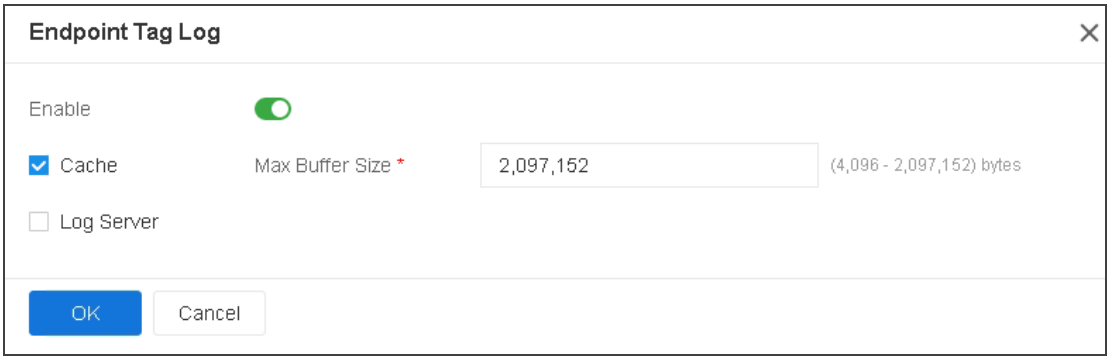
Endpoint Tag Log

The system support management of endpoint tag logs by using the endpoint tag log function. To configure and manage endpoint tag logs, take the following steps:

1. Select **Monitor** > **Log** > **Endpoint Tag Log** or select **ZTNA** > **Endpoint Tag Log**.
    - Time: indicates the endpoint tag log's generation time.
    - Type: indicates the endpoint tag log type, including login, logout, abnormal logout, endpoint tag update and application resource update.
    - User Name: indicates the user name.
    - User IP: indicates the user IP address.
    - AAA Server: indicates the AAA server to which the user belongs.
    - Endpoint Name: indicates the endpoint name.
    - Endpoint IP: indicates the endpoint IP address.
    - OS: indicates the operating system of the endpoint.
    - Endpoint Tags: indicates the endpoint tag associated with the user.

- ZTNA Server: indicates the ZTNA service name that the user accesses.
- Allowed Application Resources: indicates the application resources that the user are allowed to access.
- Denied Application Resources: indicates the application resources that the user are not allowed to access.

2. Click **Configure** and enter the **Endpoint Tag Log** page.



Option	Description
Enable	Click the button to enable the endpoint tag log function and select the destinations where the endpoint tag logs will be sent to. You can select multiple destinations. By default, the endpoint tag log function is enabled and the logs will be sent to the memory buffer.
Cache	Select the check box to send endpoint tag logs to the memory buffer.
Max Buffer Size	When configuring the system to send endpoint tag logs to the memory buffer, you can define the memory buffer size for storing the endpoint tag logs. The range is 4096 to 2097152, in bytes. The default value is 2097152.

Option	Description
Log Server	Select the check box to send endpoint tag logs to the syslog server, in plaintext. You need to configure a syslog server first. Click the "" link to view all syslog servers that have been configured. For configuration information about syslog server, refer to Creating a Log Server.

3. Click **Filter** to view endpoint tag logs that match the specified filtering conditions.
4. Click **Clear** to clear all endpoint tag logs.

   Note: This option is not supported for devices that support sending log information to the local database.
5. Click **Export** to export all endpoint tag logs to a local file.

Managing Logs

You can configure system to enable the logging function, including enabling various logs.

Configuring Logs

To configure parameters of various log types, take the following steps:

1. Select **Monitor > Log > Log Management**.
2. Click the **Enable** button of the log type that you want, and click the  button to enter the corresponding log settings.
3. Click **OK**.

Option Descriptions of Various Log Types

This section describes the options when you set the properties of each log types.

Event Log

Option	Description
Enable	Click the button to enable the event logging function.
Console	Select the check box to send a syslog to the Console. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Terminal	Select the check box to send a syslog to the terminal. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Cache	Select the check box to send a syslog to the cache. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max Buffer Size - The maximum size of the cached logs. The default value may vary for different hardware platforms.
File	Select the check box to send a syslog to a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box.
Log Server	Select the check box to export event logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add new server. • Lowest Severity - Specifies the lowest severity level. Logs

Option	Description
	below the severity level selected here will not be exported.
Email Address	Select the check box to send event logs to the email. • View Email Address: Click to see all existing email addresses or add a new address. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
SMS	Select the check box to send event logs to the SMS. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.

Network Log

Option	Description
Enable	Click the button to enable the network logging function.
Cache	Select the check box to export network logs to the cache. • Max Buffer Size - The maximum size of the cached network logs. The value range is 4096 to 524288 bytes. The default value may vary for different hardware platforms.
File	Select the check box to send a syslog to a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box.

Option	Description
Log Server	Select the check box to export network logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server.
Local DB	Select the check box to send network logs to the local database. Note: A-series firewalls installed with hard disks support this function.

Configuration Log

Option	Description
Enable	Click the button to enable the configuration logging function.
Cache	Select the check box to export configuration logs to the cache. • Max Buffer Size - The maximum size of the cached configuration logs. The value range is 4096 to 524288 bytes. The default value may vary for different hardware platforms.
File	Select the check box to send configuration logs to a file. • Max File Size - Specifies the maximum size of the configuration log file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the network log file into the File Name box.
Log Server	Select the check box to export network logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add new server.
Log Speed	Select the check box to define the maximum efficiency of generating

Option	Description
Limit	logs. • Maximum Speed - Specified the speed (messages per second).
Local DB	Select the check box to send configuration logs to the local database. Note: A-series firewalls installed with hard disks support this function.

Session Log

Option	Description
Enable	Click the button to enable the session logging function. • Record User Name: Select to show the user's name in the session log messages. • Record Host Name: Select to show the host's name in the session log messages.
Cache	Select the check box to export session logs to cache. • Max Buffer Size - The maximum size of the cached session logs. The value range is 4096 to 2097152 bytes. The default value may vary for different hardware platforms.
Local DB	Select the check box to send session logs to the local database. Note: A-series firewalls installed with hard disks support this function.
Log Server	Select the check box to export session logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you

Option	Description
	will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

PBR Log

Option	Description
Enable	Click the button to enable a PBR logging function. • Record User Name: Select to show the user's name in the PBR log messages. • Record Host Name: Select to show the host's name in the PBR log messages.
Cache	Select the check box to export PBR logs to the cache. • Max Buffer Size - The maximum size of the cached PBR logs. The value range is 4096 to 2097152 bytes. The default value may vary for different hardware platforms.
Log Server	Select the check box to export PBR logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of plain text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

NAT Log

Option	Description
Enable	Click the button to enable the NAT logging function. • Record Host Name: Select to show the host's name in the NAT log messages.
Cache	Select the check box to export NAT logs to cache. • Max Buffer Size - The maximum size of the cached NAT logs. The default value may vary for different hardware platforms.
Local DB	Select the check box to send NAT logs to the local database. Note: A-series firewalls installed with hard disks support this function.
Log Server	Select the check box to export NAT logs to log servers. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

IoT Log

Option	Description
Enable	Click the button to enable the IoT logging function. • Record Host Name: Select to show the host's name in the IoT log messages.
Cache	Select the check box to export IoT logs to cache. • Max Buffer Size - The maximum size of the cached IoT logs.

Option	Description
Log Server	Select the check box to export IoT logs to log servers. • View Log Server - Click to see all existing servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

EPP Log

Option	Description
Enable	Click the button to enable the EPP logging function.
Terminal	Select the check box to send a syslog to the terminal. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Cache	Select the check box to export EPP logs to cache. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max Buffer Size - The maximum size of the cached logs.
File	Select the check box to send EPP logs to a file. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max File Size - Specifies the maximum size of the EPP log

Option	Description
	file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes.
Log Server	Select the check box to export EPP logs to log servers. • View Log Server - Click to see all existing servers or to add a new server. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.
Email Address	Select the check box to send EPP logs to the email. • View Email Address: Click to see all existing email addresses or add a new address. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.

URL Log

Option	Description
Enable	Click the button to enable the URL logging function. • Record Host Name: Select to show the host's name in the URL log messages.
Cache	Select the check box to export URL logs to the cache.

Option	Description
	• Max Buffer Size - The maximum size of the cached URL logs. The default value may vary for different hardware platforms.
Log Server	Select the check box to export URL logs to a log server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

File Filter Log

Option	Description
Enable	Click the button to enable the File Filter logging function.
Cache	Select the check box to export File Filter logs to cache. • Max Buffer Size - The maximum size of the cached File Filter logs. The default value may vary for different hardware platforms.
Log Server	Select the check box to export File Filter logs to log server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can

Option	Description
	be Round Robin or Src IP Hash.

Content Filtering Log

Option	Description
Enable	Click the button to enable the Content Filter logging function.
Cache	Select the check box to export Content Filter logs to cache. • Max Buffer Size - The maximum size of the cached Content Filter logs. The default value may vary for different hardware platforms.
Log Server	Select the check box to export Content Filter logs to log server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

Network Behavior Record Log

Option	Description
Enable	Click the button to enable the Network Behavior Record logging function.
Cache	Select the check box to export Network Behavior Record logs to cache. • Max Buffer Size - The maximum size of the cached Network Behavior Record logs. The default value may vary from dif-

Option	Description
	ferent hardware platforms.
Log Server	Select the check box to export Network Behavior Record logs to log server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.

CloudSandBox Log

Option	Description
Enable	Click the button to enable the CloudSandBox logging function.
Cache	Select the check box to export CloudSandBox logs to the cache. • Max Buffer Size - The maximum size of the cached CloudSandBox logs.
Local DB	Select the check box to send cloud sandbox logs to the local database. Note: A-series firewalls installed with hard disks support this function.
File	Select to export CloudSandBox logs as a file. • Max File Size - Specifies the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes.

Option	Description
	• Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the File Name box.
Log Server	Select the check box to export CloudSandBox logs to log server. • View Log Server - Click to see all existing syslog servers or to add a new server.

Threat Log

Option	Description
Enable	Click the button to enable the threat logging function. • Record User Name: Select to show the user's name in the threat log messages.
Record User Information	Click the button to enable the Record User Information function for Threat Log. With this function enabled, threat logs will record information about the authenticated user, including AAA server, username, and hostname.
Cache	Select the check box to export threat logs to the cache. • Max buffer size - The maximum size of the cached threat logs. The default value may vary from different hardware platforms. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported.
Local DB	Select the check box to export threat logs to local database. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. Note: A-series firewalls installed with hard disks support this function.

Option	Description
File	Select to export threat logs as a file to USB. • Lowest Severity - Specifies the lowest severity level. Logs below the severity level selected here will not be exported. • Max File Size - Exported log file maximum size. • Save logs to USB - Select a USB device and enter a name as the log file name.
Terminal	Select to send logs to terminals.
Log Server	Select the check box to export threat logs to log server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - the distributed logs can be in the format of binary or text. If you select the check box, you will send log messages to different log servers, which will relieve the pressure of a single log server. The algorithm can be Round Robin or Src IP Hash.
Email address	Select the check box to export logs to the specified email address. • Viewing Email Address: Click to see or add email address.
Database	Select the checkbox to save logs in the local device. Only several platforms support this parameters. • Disk Space - Enter a number as the percentage of a storage the logs will take. For example, if you enter 30, the threat logs will take at most 30% of the total disk size.

Option	Description
	• Disk Space Limit - If **Auto Overwrite** is selected, the logs which exceed the disk space will overwrite the old logs automatically. If **Stop Storing** is selected, system will stop storing new logs when the logs exceed the disk space.

Share Access Log

Option	Description
Enable	Click the button to enable the Share Access logging function.
Console	Select to export Share Access logs to the console.
Cache	Select the check box to export Share Access logs to the cache. • Max buffer size - The maximum size of the cached Share Access logs.
Log Server	Select the check box to export Share Access logs to log server. • View Log Server - Click to see all existing syslog servers or to add a new server.

Endpoint Tag Log

Option	Description
Enable	Click the button to enable the endpoint tag log function and select the destinations where the endpoint tag logs will be sent to. You can select multiple destinations. By default, the endpoint tag log function is enabled and the logs will be sent to the memory buffer.
Console	Select to export Share Access logs to the console.
Cache	Select the check box to send endpoint tag logs to the memory buffer. • Max Buffer Size - Specify the memory buffer size for storing

Option	Description
	the endpoint tag logs. The range is 4096 to 2097152, in bytes. The default value is 2097152.
Local DB	Select the check box to send endpoint tag logs to the local database. Note: A-series firewalls installed with hard disks support this function.
Log Server	Select the check box to send endpoint tag logs to the syslog server, in plaintext. You need to configure a syslog server first. Click the "View Log Server" link to view all syslog servers that have been configured. For configuration information about syslog server, refer to Creating a Log Server.

Log Configuration

You can create log server, set up log email address, add UNIX servers and configure sending sourceport .

Configuring a Log Server

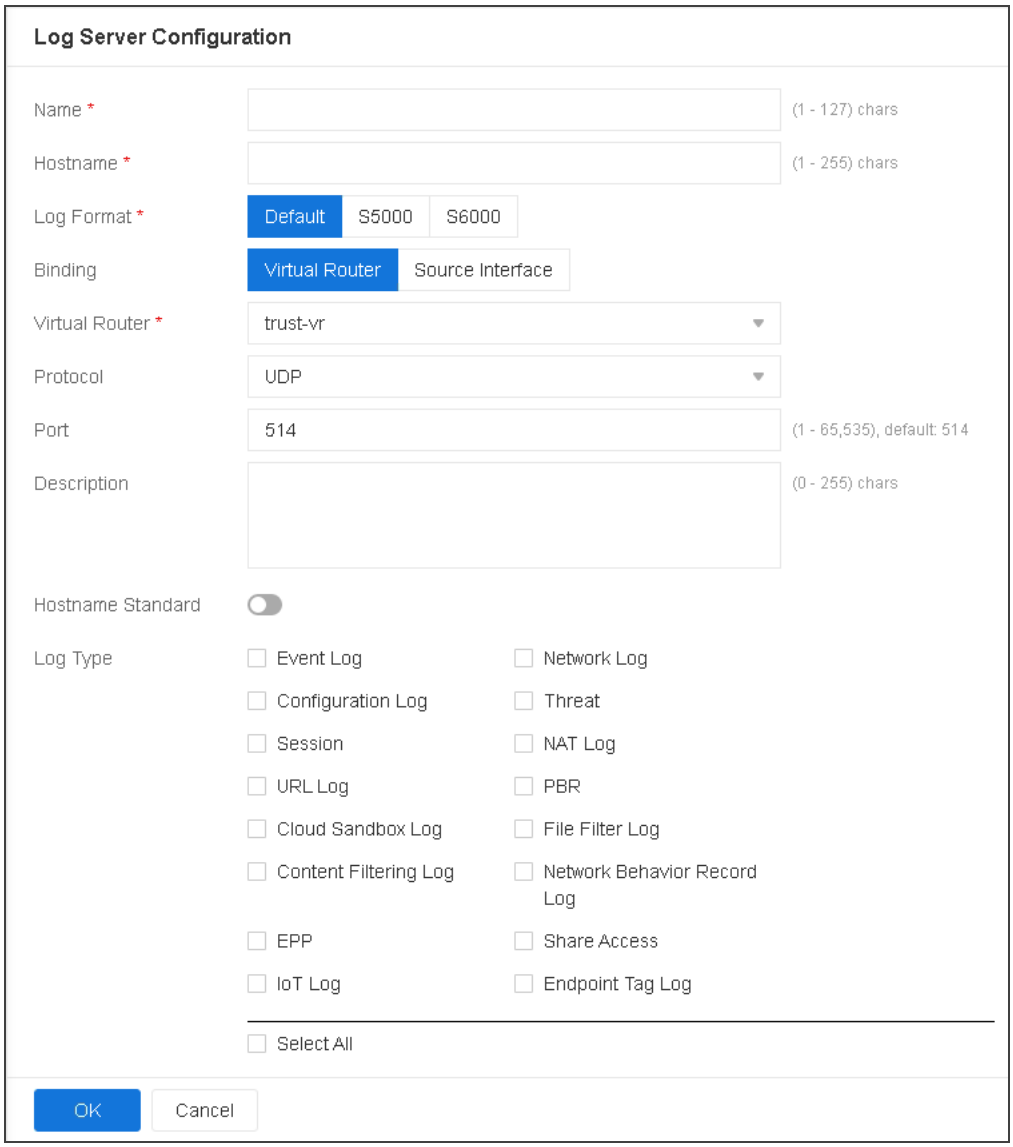
In the **Log Server Configuration** tab, you can create, edit, or delete the log server that is used for receiving logs. In addition, you can configure the sending sourceport number and log encoding.

Creating a Log Server

To create a log server, take the following steps:

1. Select **Monitor > Log > Log Configuration**.
2. Click **Log Server Configuration** tab.

3. Click **New**.



Option	Description
Name	Specifies the name of the log server, which needs to be 1 to 127 characters in length.
Hostname	Specifies the IP address or host name of the log server.
Log Format	Specifies the log format of Syslog Server log Server, including Default, SGCC S5000 and SGCC S6000. Select the format

Option	Description
	according to the log Server type. • Default - Syslog Server log Server can only receive the Hillstone log format. • S5000 - Syslog Server log Server can only receive SGCC-S5000 log format, such as the log Server's of State Grid Corporation of China. • S6000 - Syslog Server log Server can only receive SGCC-6000 log format, such as the monitoring Server's of State Grid Corporation of China.
Binding	Specifies the source IP address to receive logs. • Virtual Router: Select **Virtual Router** and then select a virtual router form the drop-down list. If a virtual router is selected, the device will determine the source IP address by searching the reachable routes in the virtual router. • Source Interface: Select **Source Interface** and then select a source interface from the drop-down list. The device will use the IP address of the interface as the source IP to send logs to the syslog server. If management IP address is configured on the interface, the management IP address will be preferred.
Protocol	Specifies the protocol type of the syslog server. The Secure-TCP uses the TLS encryption protocol. If "Secure-TCP" is selected, you can select **Do not validate the server certificate** option, and

Option	Description
	system can transfer logs normally and do not need any certifications.
Port	Specifies the port number of the syslog server.
Hostname Standard	By default, the logs sent to the Syslog Server does not display the year, the hostname and the log severity, i.e. **<Device Number*8+log severity> date/timeSN(VSYS name) log ID HillstoneNetworks#log type@module: descriptions**. With this option checked, the logs sent to the Syslog Server displays the hostname and does not display the device SN, the format is: **<Device Number*8+log severity> date/timehostname log ID HillstoneNetworks#log type@module: descriptions**.
Description	Enter a description for the syslog server as needed, which can be up to 255 characters in length.
Log Type	Specifies the log types the syslog server will receive.

4. Click **OK** to save the settings.

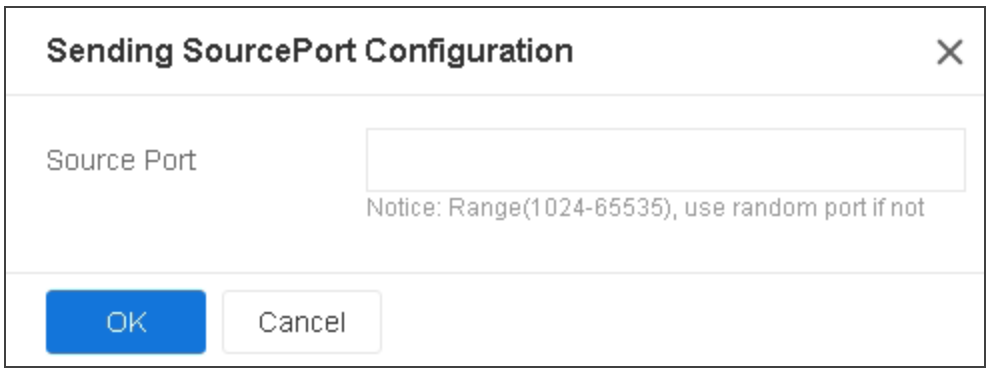
Notes: You can add at most 15 log servers.

Configuring Sending Souceport Number

The system supports to specify the sending sourceport number used to send log messages to the Syslog Server. When the sending sourceport number is specified, the system will use the specified sending sourceport to send log messages to the Syslog Server. If the sending sourceport number is not specified, the system will use the random sourceport to send log messages to the Syslog Server by default.

To configure sending souceport number, take the following steps:

1. Click **Monitor > Log > Log Configuration** and select the Log Server Configuration tab.
2. Click the **Sending Sourceport Configuration** button to open the Sending Sourceport Configuration page.



3. Enter the specified sourceport number. The range is from 1024 to 65535. If you want to cancel the configuration of the current sourceport number, delete the value.
4. Click **OK**.

Notes:

- The binary logs sent to the Syslog Server is not influenced by the sending sourceport configuration. The binary logs are sent by UDP protocol using 5566 sourceport.
- When SNAT is enabled, the system will randomly select port as the sending sourceport according to the port resources of network addresses translated by NAT.

Configuring Log Encoding

The default encoding format for the log information that is output to the log server is utf-8, and the user can start GBK encoding as needed. After the GBK encoding format is opened, the log encoding format that is output to the log server will be GBK encoding. To enable the GBK encoding :

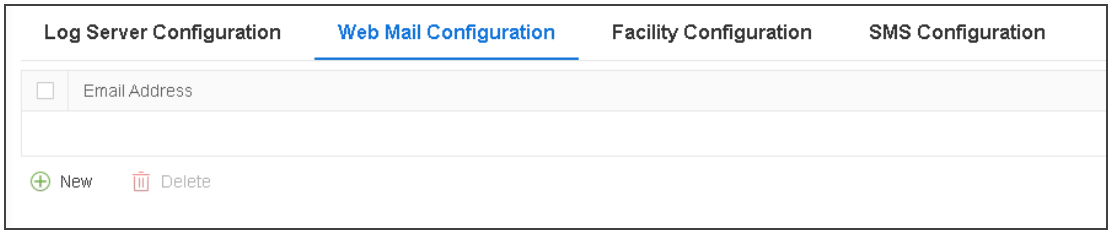
1. Select **Monitor > Log > Log Configuration**.
2. Click **Log Server Configuration** tab.
3. Click the **Log Encoding Configuration** button in the upper right corner to open the Log Encoding Configuration page.
4. Click the button to enable the GBK Encoding.
5. .Click **OK** to save the settings.

Adding Email Address to Receive Logs

An email in the log management setting is an email address for receiving log messages.

To add an email address, take the following steps:

1. Select **Monitor > Log > Log Configuration**.
2. Click **Web Mail Configuration** tab.



3. Enter an email address and click **New**.
4. If you want to delete an existing email, click **Delete**.

Notes: You can add at most 3 email addresses.

Facility Configuration

The system supports to configure the facility generating log information. When the log information is sent to the log server, the Facility field in the log server will display the facility. You can

globally configure the facility generating log information, or separately specify the facility generating event logs and traffic logs. In addition, the separately specified facility takes precedence over the globally configured facility. If not configured, the Facility field defaults to "local7".

To configure a facility, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration**.
2. In the **Facility Configuration** tab, configure the following options:

Option	Description
Global Configuration (required)	Select the facility that generates all types of logs from the drop-down list. Default value: local7. This is the global configuration, which can take effect for all types of logs.
event	Select the facility that generates event logs from the drop-down list. If not specified, the globally configured facility is used.
traffic	Select the facility that generates traffic logs from the drop-down list. If not specified, the globally configured facility is used.

3. Click **OK**.

Specifying a Mobile Phone

To specify a mobile phone to receive logs, take the following steps:

1. Select **Monitor > Log > Log Configuration**.
2. Click **SMS Configuration** tab.
3. The SMS Send Type field displays the selected type of sending SMS messages. To configure the type, click **configuration**.
    - SMS Send Type: Select **SMS Modem**, **SMS Gateway**, or None. None indicates that the function of sending logs by SMS is disabled.

- SMS Gateway: If **SMS Gateway** is selected, you need to select a configured SMS gateway name from the drop-down list, or click ⊕ to create an SMS gateway.

4. Enter a mobile phone number and click **New**.
5. If you want to delete an existing mobile phone number, click **Delete**.



Notes: You can add at most 3 mobile phone numbers.

Reporting

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

System provides rich and vivid reports that allow you to analyze network risk, network access and device status comprehensively by all-around and multi-dimensional statistics and charts.

You can configure report task in "Report Template" on Page 1610 and "Report Task" on Page 1616, and view generated report files in "Report File" on Page 1609.

Related Topics:

- "Report File" on Page 1609
- "Report Template" on Page 1610
- "Report Task" on Page 1616
- "Report Status" on Page 1623

Report File

Go to **Monitor > Reports > Report File** and the report file page shows all of the generated report files.



- Sort report files by different conditions: Select **Group by Time**, **Group by Task** or **Group by Status** from the drop-down list, and then select a time, task or status from the selective table, and the related report files will be shown in the report file table.
- The bold black entry indicates that the report file status is "unread".
- Click **Delete** to delete the selected report files.
- Click **Export** , the browser launches the default download tool, and downloads the selected report file.
- Click **Mark as Read** to modify the status of the selected report files.
- Click Filter to select the condition in the drop-down list. Search for specific report files based on filter condition.
- In the File Type column, click the icon of the report file to preview the report file. Not all platforms support this function.

Notes: If your browser has enabled "Blocking pop-up windows", you will not see the generated file. Make sure to set your browser "Always allow pop-up windows", or you can go to your blocked window history to find the report file.

Report Template

Report templates, define all the contents in the report files. To generate the report file, you need to configure the report template first.

Report templates are classified as predefined and user-defined templates, providing a variety of pre-categorized report items.

- Predefined Template: Predefined templates are built in system. By default, different report items have been selected for each predefined template category. The predefined template cannot be edited or deleted. The predefined template categories are as follows:

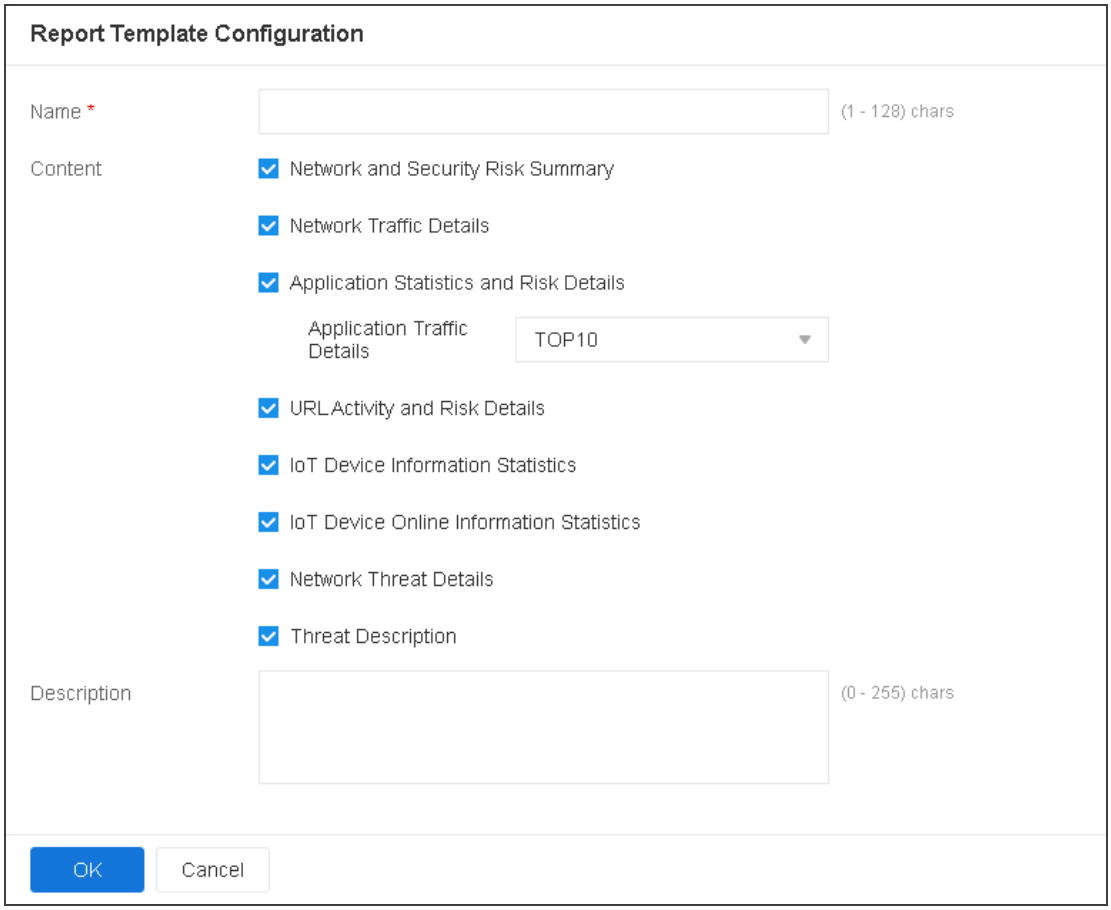
Category	Description
Global Network and Risk Assessment Report	Statistics of the global network and risk status, covering the overview, network and application traffic, network threats and host details.
Network and Application Traffic Report	Statistics of the current network situation, covering the network traffic, application traffic and URL hits.
Network Threat Report	Statistics of the threats in the current network, covering the threat trend, external attackers and threat categories.
IoT Device Report	Statistics of the current IoT device situation, covering the number of devices, the manufacturer, the type, the online status, and the traffic size.

- User-defined Template: The report template created as needed. You can select the report items. Up to 32 user-defined templates can be created.

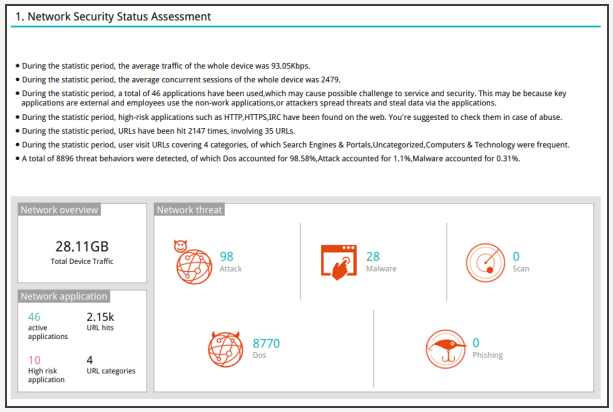
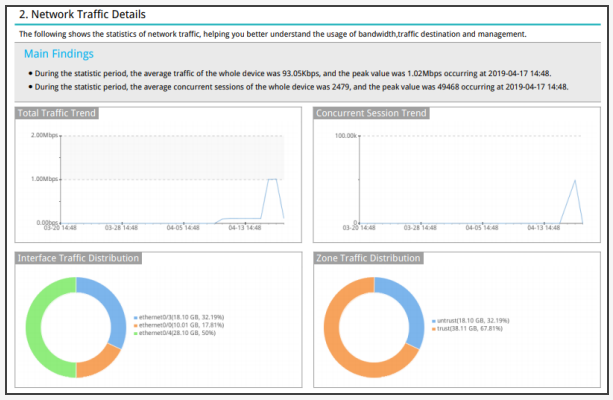
Creating a User-defined Template

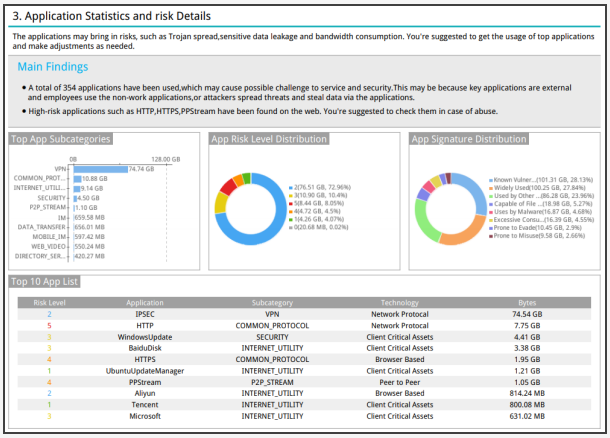
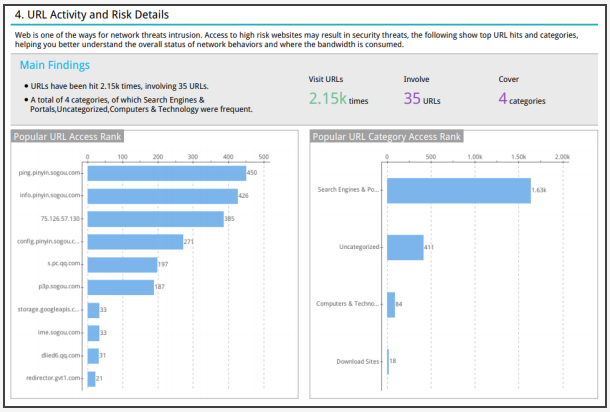
To create a user-defined template, take the following steps:

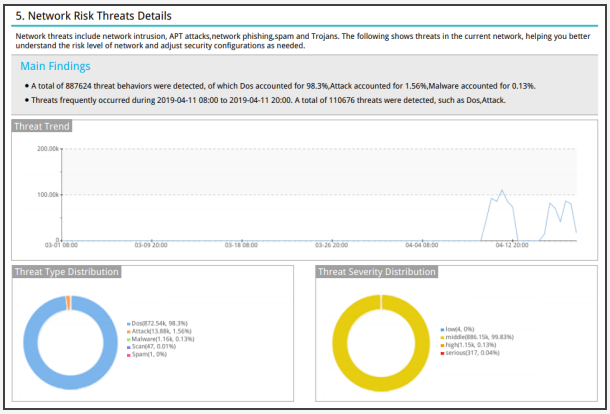
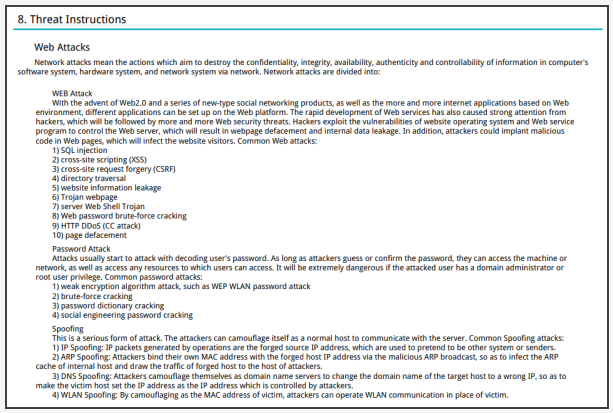
1. Click **Monitor > Reports > Template**.
2. Click **New**.



Option	Description
Name	Specifies the name of the report template.
Content	Select the check box of the report item as needed. By default, all report items are selected. The report items are described as follows: • Network and Security Risk Summary: Statistics of the comprehensive and overall assessment for the health status and security risks of the entire network.

Option	Description
	 • Network Traffic Details: Statistics of network traffic, helping you better understand the usage of bandwidth, traffic destination and management.  • Application Statistics and Risk Details: Statistics of the traffic of all applications on the device and obtains the usage of the main service applications in the intranet. Click the **TOP** drop-down list to specify the number of applications that need to count the traffic for ranking, including TOP5, TOP10, TOP20 and TOP50.

Option	Description
	 • URL Activity and Risk Details: Statistics of device URL access trends and rankings.  • Network Threat Details: Statistics of the threat events detected by the device, the distribution of external attacks, etc., in order to know the network threats and risks existing in the current network.

Option	Description
	 • Threat Description: Display the detailed description of the threat, helping understand the threat information. 
Description	Specifies the description of the report template.

3. Click **OK** to complete user-defined template configurations.

Editing a User-defined Template

To edit a user-defined report template, take the following steps:

1. Click **Monitor > Reports > Template**.

2. In the templates list, select the user-defined report template entry that needs to be edited.

3. Click **Edit**.
4. Click **OK** to save the settings.

Deleting a User-defined Template

To delete a user-defined report template, take the following steps:

1. Click **Monitor > Reports > Template**.
2. In the templates list, select the user-defined report template entry that needs to be deleted.
3. Click **Delete**.

Cloning a Report Template

System supports the rapid clone of a report template. You can clone and generate a new report template by modifying some parameters of one current report template.

To clone a report template, take the following steps:

1. Click **Monitor > Reports > Template**.
2. In the templates list, select a report template that needs to be cloned.
3. Click the **Clone** button above the list, and in the **Report Template Configuration** page, enter the newly cloned report template name into the "Name" .
4. The cloned report template will be generated in the list.

Report Task

The report task is the schedule related to report file. It defines the report template, data range, generation period, generation time, and the output method of report files.

You can configure report tasks and generate report files on the device according to your needs.

Creating a Report Task

To create a report task, take the following steps:

1. Select **Monitor> Reports> Report Task**.
2. Click **New**.

   In this page, configure the values of report task.

Option	Description
Name	Specifies the name of the report task.
Description	Specifies the description of the report task. You can modify it according to your requirements.

Expand Report Template, select the report template you want to use for the report task.

Option	Description
Report Template	Specifies the report template to be used by the report task: 1. Select the report template (predefined report template or created user-defined report template) from the **Report Template** list on the left. 2. When the report template is selected, the selected report template list shows the description of the template and the details of the report item on the right. You can also click **New** or **Edit** button in the **Report Template** list on the left to open the **Report Template Configuration** page and create or edit a user-defined report template quickly.

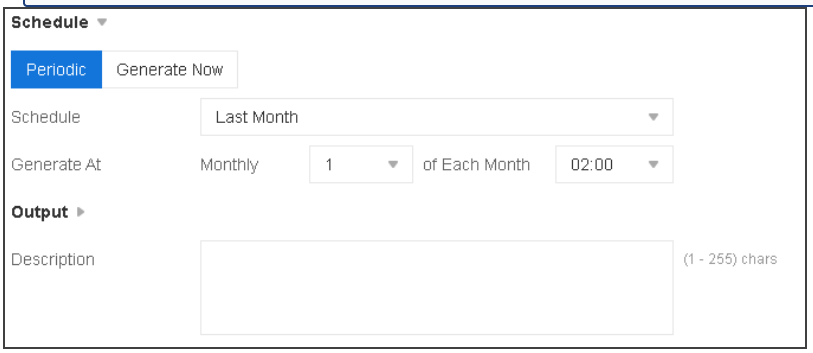


Expand Threat Data Range

Option	Description
Threat Type	Specifies the type of threat to generate report statistics. There are six threat types, which are Scan, Attack, Dos, Phishing, Spam, and Malware.
Severity	Specifies the threat level for generating report statistics. The threat level can be Critical, High, Medium, or Low.
Zone	Specifies the security zone of the report statistics. 1. Click + of the **Zone** drop-down list. 2. Specifies the zone from the **Zone** list that appears on the right. • To modify the configuration of a zone, hover your mouse over the zone entry and then click to go to the **Zone Configuration** page. • To create a new zone, click to go to the **Zone Configuration** page.
Interface	Specifies the interface of the report statistics. 1. Click + of the **Interface** drop-down list.

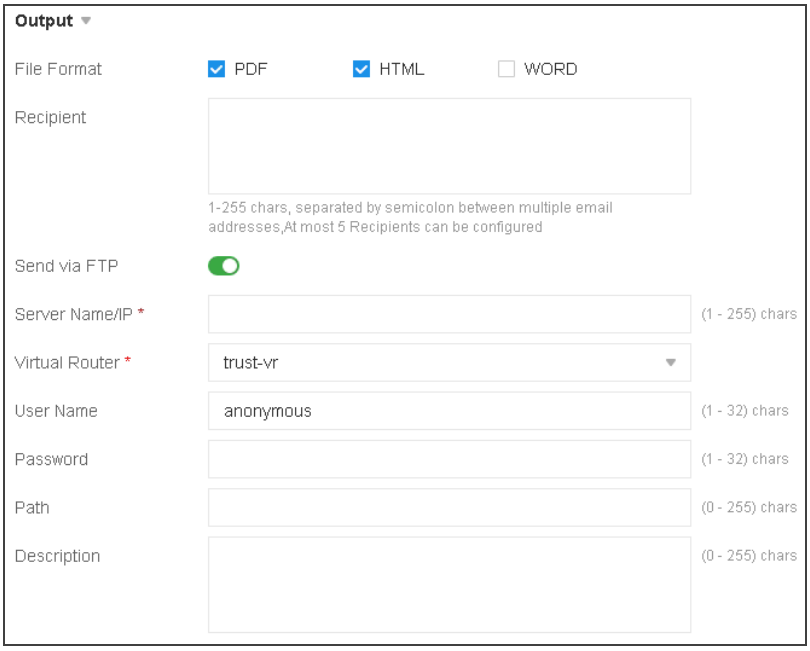
Option	Description
	2. Specifies the interface from the **Interface** list that appears on the right. • To modify the configuration of an interface, hover your mouse over the interface entry and then click  to go to the **Ethernet Interface** page. • To create a new zone, click  to go to the **Ethernet Interface** page.
IP	Specifies the IP range for generating report statistics. The IP range can include both source IP address and destination IP address. 1. Click + of the **IP** drop-down list. 2. Select the IP address type from the **IP** list that appears on the right, including IP/Netmaskand IP Range. 3. Enter the required address of the address type. 4. Click **Add** to add the addresses to the right pane. 5. After adding the desired addresses, click **Close** to complete the configuration. 6. If you need to delete the added address, select the address you want to delete in the right pane, and click .

Notes: This configuration item is supported only by devices with hard disks.



Expand Schedule, configure the running time of the report task.

Option	Description
Schedule	The schedule specifies the running time of the report task. The report task can be run periodically or run immediately. Periodic: Generates report files as planned. • Schedule: Specifies the statistical period - last day, last month. • Generate At: Specifies the generation time. Generate Now: Generates report files immediately. • Specifies the start time and end time of absolute statistical period in the time text box. This configuration item is supported only by devices with hard disks. • Type: Generates report file based on the data in the specified statistical period.



Expand Output, configure the output mode information of the report.

Option	Description
File Format	Specifies the output format of the report file, including PDF, HTML, and WORD formats.
Recipient	Sends report file via email. To add recipients, enter the email addresses in to the recipient text box (use ";" to separate multiple email addresses. Up to 5 recipients can be configured).
Send via FTP	Click the **Enable** button to send the report file to a specified FTP server. • Server Name/IP: Specifies the FTP server name or the IP address. • Virtual Router: Specifies the virtual router of the FTP server from the drop-down list. To create a new virtual router, click the drop-down list and then click ⊕ on the

Option	Description
	expanded virtual router list to go to the **Virtual Router Configuration** page. • Username: Specifies the username used to log on to the FTP server. • Password: Enter the password of the FTP username. • Anonymous: Select the check box to log on to the FTP server anonymously. • Path: Specifies the location where the report file will be saved.

3. Click **OK**.

Editing the Report Task

To edit the report task, take the following steps:

1. Select **Monitor > Reports > Report Task**.
2. In the report task list, select the report task entry that needs to be edited.
3. Click the **Edit** button on the top to open the **Report Task Configuration** page to edit the selected report task.
4. Click **OK** to save the settings.

Deleting the Report Task

To delete the report task, take the following steps:

1. Select **Monitor > Reports > Report Task**.
2. In the report task list, select the report task entry that needs to be deleted.
3. Click the **Delete** button on the top to delete the selected report task.

Enabling/Disabling the Report Task

To enable or disable the report task, take the following steps:

1. Select **Monitor > Reports > Report Task**.
2. Select the task, and click the **Enable** or **Disable** button on the top.

   By default, the user-defined task is enabled.

Report Status

The generation of a report might take a long time. You can view the running status of report tasks on the Report Status page. You can view the status of an immediate report task as soon as it is created. For a periodic report task, you can the status of it when the execution time reaches.

Select **Monitor** > **Report** > **Report Status**, click **Processing** to view the status of current report tasks.

- Time: indicates the time used by executing the report task.
- Name: indicates the name of the report task.
- Status: indicates the status of the report task, including "waiting", "generating" and "complete".
- Stop: click **Stop** after selecting a report task to terminate its execution.

Select **Monitor** > **Report** > **Report Status**, click **Failed** to view the report tasks that fail to be executed.

- Time: indicates the time when the report task execution ends.
- Name: indicates the name of the report task.
- Status: indicates the status of the report task. For reports that fail to be executed, the status is "Failed".
- Fail Cause: indicates the cause of execution failure.

NetFlow

NetFlow is a data exchange method, which records the source /destination address and port numbers of data packets in the network. It is an important method for network traffic statistics and analysis.

Hillstone NetFlow supports the NetFlow Version 9. With this function configured, the device can collect user's ingress traffic according to the NetFlow profile, and send it to the server with NetFlow data analysis tool, so as to detect, monitor and charge traffic.

Related Topics:

- "Configuring NetFlow" on Page 1624

Configuring NetFlow

The NetFlow configurations are based on interfaces.

To configure the interface-based NetFlow, take the following steps:

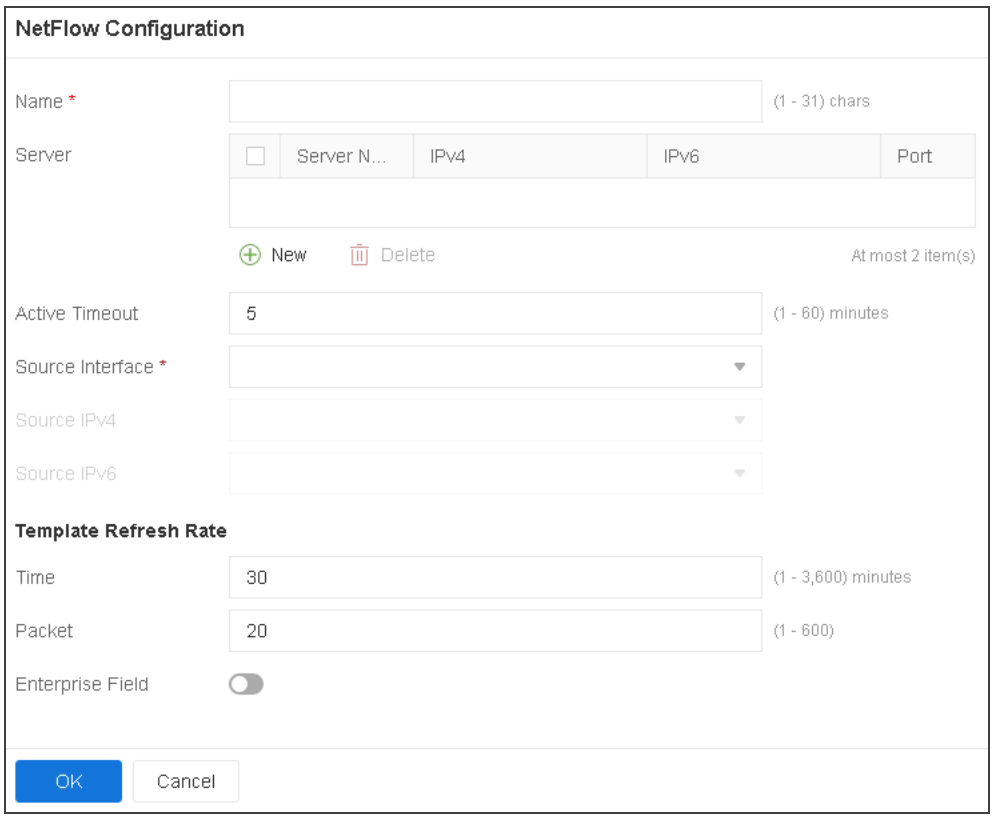
1. Click **Object > NetFlow > Configuration**. Select **Enable** check box to enable the NetFlow function.
2. Click **Object > NetFlow > Profile** to create a NetFlow rule .
3. Bind the NetFlow rule to an interface. Click **Network > Interface**. Select the interface you want to bind or click **New** to create a new interface. In the Interface Configuration dialog

box, select the **Basic** tab and then select a NetFlow rule from the **NetFlow configuration** drop-down list.

Configuring a NetFlow Rule

To configure the NetFlow rule, take the following steps:

1. Click **Object > NetFlow > Profile**.
2. Click **New** to create a new NetFlow rule. To edit an existing one, select the check box of this rule and then click **Edit**.



Option	Description
Name	Enter the name of the NetFlow rule.
Server	To configure the NetFlow server, take the following steps:

Option	Description
	1. Type the server name, IP address and port number into the **Server Name**, **IPv4**, **IPv6**, and **Port** box respectively. 2. Click **New** to add a NetFlow server which will be displayed in the list below. 3. Repeat the above steps to add more servers. You can add up to 2 servers. To delete a server, select the server check box you want to delete from the list and click **Delete**.
Active Timeout	The active timeout value is the time after which the device will send the collected NetFlow traffic information to the specified server once. Type the active timeout value into the **Active Timeout** box. The range is 1 to 60 minutes. The default value is 5 minutes.
Source Interface	Select the source interface for sending NetFlow traffic information in the **Source Interface** drop-down list.
Source IPv4	After specifying the source interface, the system will automatically acquire and display the management IPv4 address or the secondary IPv4 address of the source interface from the drop-down list.
Source IPv6	After specifying the source interface, the system will automatically acquire and display the IPv6 address of the source interface.

Option	Description
Template Refresh Rate	You can configure the NetFlow template refresh rate by time or number of packets, after which system will refreshes the NetFlow rule. • Time: Specifies the time after which system refreshes the NetFlow rule. The range is 1 to 3600 minutes. The default value is 30 minutes. • Packets: Specifies the number of packets. When the number of NetFlow packets exceeds the specified value, system will refreshes the NetFlow rule. The range is 1 to 600. The default value is 20.
Enterprise Field	Select the **Enterprise Field** check box, and the collected NetFlow traffic information will contain enterprise field information.

3. Click **OK** to save the settings.

NetFlow Global Configurations

To configure the NetFlow global configurations, take the following steps:

1. Select **Object > NetFlow > Configuration**.
2. Select the **Open NetFlow** check box of NetFlow to enable the NetFlow function. Clear the check box to disable the NetFlow function. The NetFlow function will take effect after rebooting.

Chapter 14 Diagnostic Center

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

System supports the following diagnostic methods:

- "Packet Capture Tool" on Page 1642: Captures packets in the system. After capturing the packets, you can export them to your local disk and then analyze them using third-party tools.
- "Test Tools" on Page 1650: Test Tools: DNS Query, Ping and Traceroute can be used when troubleshooting the network.
- "Packet Loss Statistics" on Page 1628: This function can be used to collect statistics of packet loss of different functional modules, which helps you identify issues.

Packet Loss Statistics

The system supports the Packet Loss Statistics function. This function can be used to collect statistics of packet loss of different functional modules, which helps you identify issues. The detailed function is described as follows:

- Supports statistics on packet loss of functional modules. The packet loss statistics are displayed in lists, bar charts, or line charts.
- Allows you to view detailed packet loss statistics of functional modules, including the time of packet loss, 5-tuple (source IP, source port, destination IP, destination port, and protocol type), and module of packet loss.
- Allows you to manually enable the collection of 5-tuple statistics of packet loss or set the threshold to trigger packet loss statistics collection.
- Supports the storage of packet loss statistics to device disks. You can set limits on the size of the statistics storage space.

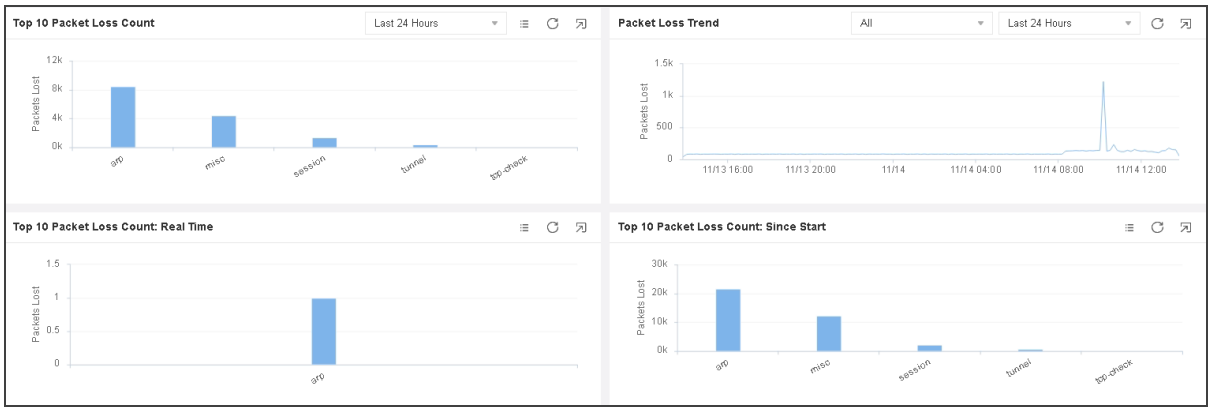
Notes: The Packet Loss Statistics function is available only for SG-6000 A-Series devices installed with hard disks.

Packet Loss Statistics

This page displays the following content

- The top 10 packet loss count of functional modules within a specified time period
- The packet loss trend of a specified functional module or all functional modules within a specified time period
- The top 10 packet loss count of functional modules in real time
- The top 10 packet loss count of functional modules since start

Select **System** > **Diagnostic Center** > **Packet Loss Statistics**:

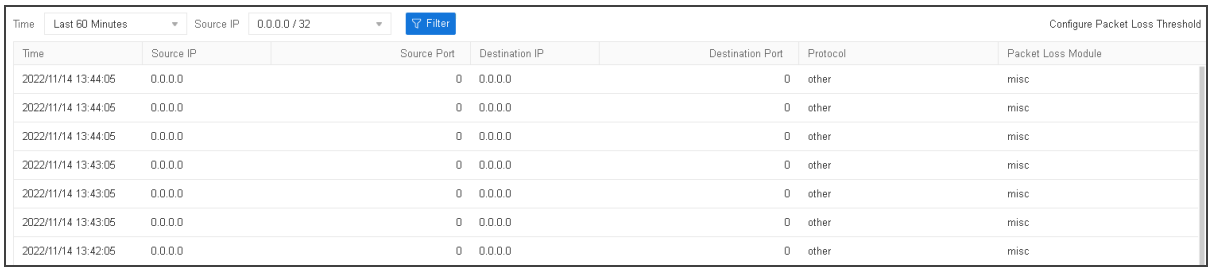


- You can view statistics in different time ranges by selecting a Statistical Period.
- Select a functional module whose statistics you want to collect from the All drop-down list in the **Packet Loss Trend** section.
- Icon and are used to switch between the list and column chart.
- Icon is used to immediately refresh statistical data on the page.

- Icon  is used to hide the current list or chart.
- Hover your mouse over the column chart or line chart to view the values of packet loss. You can click **Details** to go to the corresponding Packet Loss Details page.
- Click the name of a functional module in the list to go to its Packet Loss Details page.

Packet Loss Details

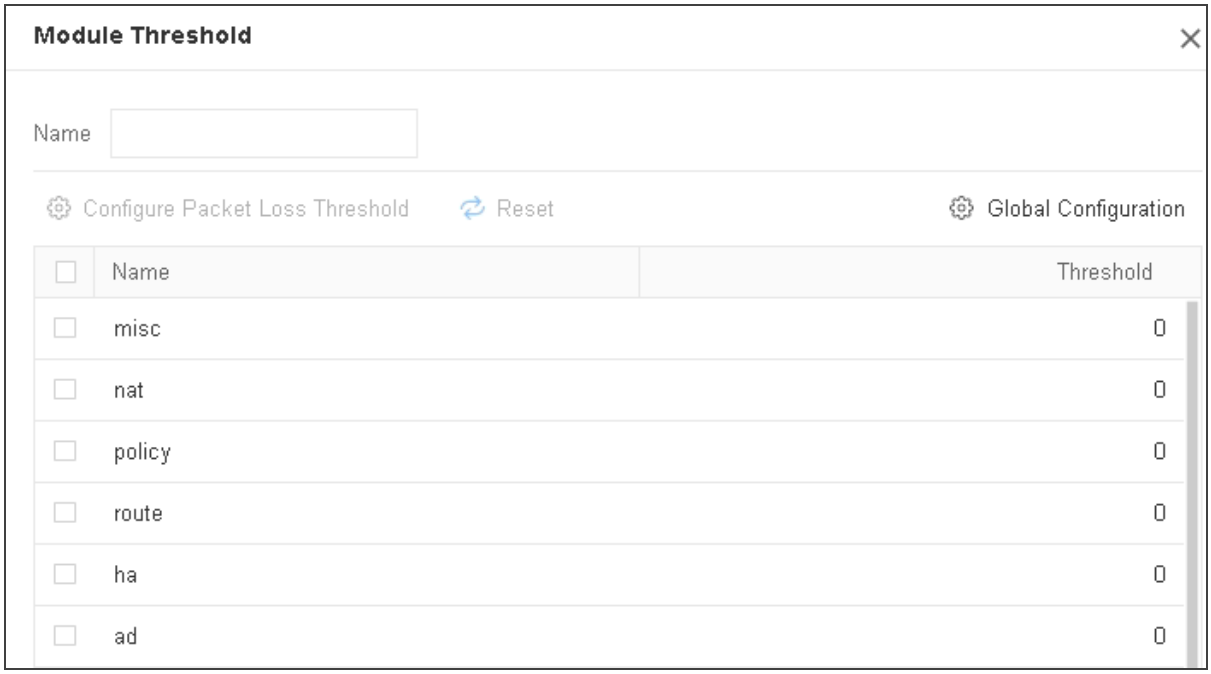
Select **System** > **Diagnostic Center** > **Packet Loss Details** to view detailed packet loss statistics of functional modules, including the time of packet loss, 5-tuple (source IP, source port, destination IP, destination port, and protocol type), and module of packet loss.



- You can view detailed packet loss statistics in different time ranges by selecting a Statistical Period.
- Click  in the upper part to specify filter conditions. The statistics that meet the filter conditions are displayed in the list.

Module Threshold

Select **System** > **Diagnostic Center** > **Packet Loss Details**, then click the **Configure Packet Loss Threshold** button on the upper right. Open the Module Threshold page, view the packet loss threshold of all functional modules.



- Enter a functional module name in the Name field to view its module threshold.
- Select a module threshold in the list and click **Configure Packet Loss Threshold**. In the **Configure Packet Loss Threshold** panel, specify a packet loss threshold for the functional module. If the packet loss count exceeds the threshold, it is determined the packet loss is abnormal and the 5-tuple of abnormal packet loss is recorded. Valid threshold values: 0 to 20000. Default value: 0, which indicates that no threshold is specified and the 5-tuple statistics of packet loss are always collected.
- Select a module threshold in the list and click **Reset** to reset the threshold to the default value of 0.
- Click **Global Configuration** in the upper-right corner of the list. In the **Global Configuration** panel, configure global settings for 5-tuple statistics of packet loss. The global configuration takes effect for all functional modules.
    - If the **5-Tuple Statistics of Packet Loss** parameter is set to **Collect upon Abnormality**, you need to enter a packet loss growth rate threshold in the field below. If the packet loss growth rate of a functional module exceeds the threshold, it

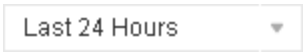
is determined that the packet loss is abnormal and the 5-tuple of abnormal packet loss is recorded. Valid threshold values: 0 to 100. Default value: 0, which indicates that no threshold is specified and the 5-tuple statistics of packet loss are always collected.

- If the **5-Tuple Statistics of Packet Loss** parameter is set to **Always Collect**, the system always records the 5-tuple statistics of packet loss of all functional modules. In this case, the packet loss threshold of functional modules and packet loss growth rate threshold do not take effect.

Packet Loss Statistics Storage Size Settings

The system allows you to store packet loss statistics to device disks. A default storage size is allocated to packet loss statistics. You can customize the storage size. For more information, see Storage Management.

Statistical Period

The system allows you to configure a statistical period. You can select a statistical period from the 

drop-down list in the upper-right corner of each statistic item or select **Custom** and customize a statistical period:

- Last 60 Minutes: displays the statistics of the last 60 minutes.
- Last 24 Hours: displays the statistics of the last 24 hours.
- Last 7 Days: displays the statistics of the last 7 days.
- Last 30 Days: displays the statistics of the last 30 days.
- Custom: Customize the statistical period. After you select this option, specify the start time and end time in the **Custom Date and Time** panel. You can specify a statistical period of at most 31 consecutive days within the last 180 days from the current date.

Packet Path Detection

This feature may not be available on all platforms. Please check your system's actual page if your device delivers this feature.

Based on the packet process flow, the packet path detection function detects the packets and shows the detection processes and results to the users with charts an descriptions. This function can detect the following packet sources: emulation packet, online packet, and imported packet (system provides the Packet Capture Tool for you that can help you capture the packets).

The detectable packets from different packet sources have different detection measures. System supports the following measures:

- Emulation packet detection: Emulate a packet and detect the process flow in the system of this packet.
- Online packet detection: Perform a real-time detection of the process flow of the packets in system.
- Imported packet detection: Import the existing packets and detect the process flow in system of the packets.

Configuring Packet Path Detection

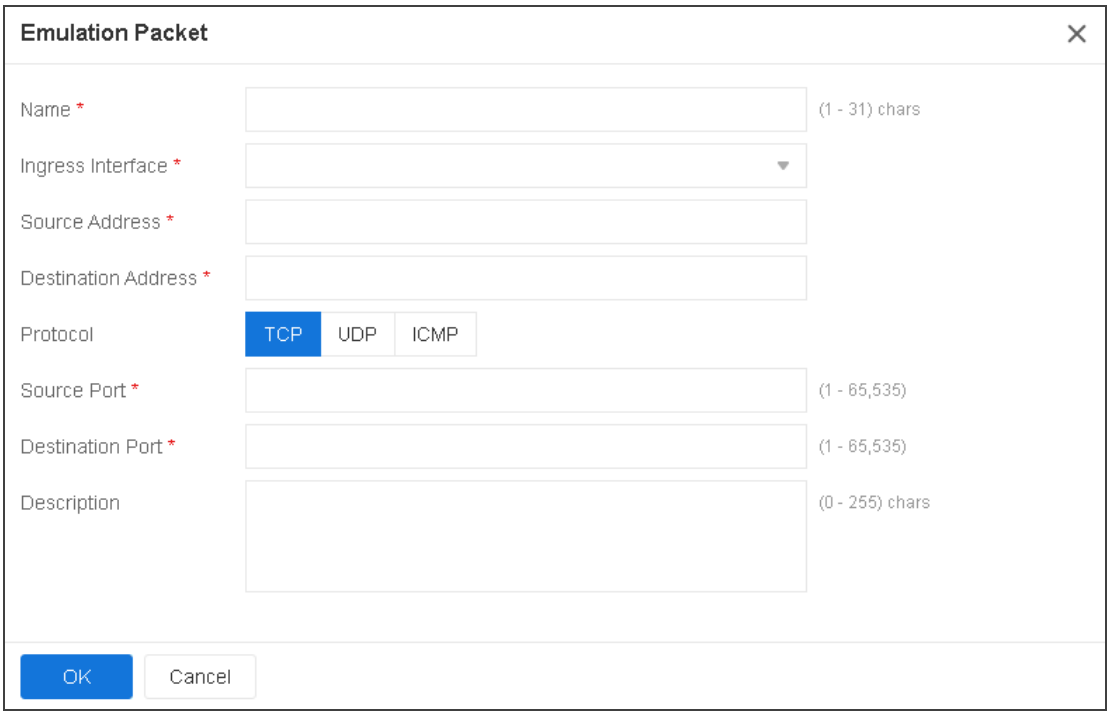
You can configure the packet path detection configurations and view the detection results in the report.

Emulation Detection

To perform the emulation detection, take the following steps:

1. Select **System > Diagnostic Center > Packet Path Detection**.
2. Click **Choose Detected Source**.

3. Click **New** , in the drop-down list, select **Emulation Packet** tab.



Option	Description
Name	Specifies the name of the emulation packet.
Ingress Interface	Select the ingress interface of the emulation packet from the drop-down list.
Source Address	Specifies the source IP address of the emulation packet in the text box.
Destination Address	Specifies the destination IP address of the emulation packet in the text box.
Protocol	Select the protocol of the emulation packet from the drop-down list. When selecting TCP or UDP, specify the source and destination ports in the Source Port and Destination Port text boxes; when selecting ICMP, enter the ICMP type and code in

Option	Description
	the Type and Value text boxes.
Description	Specifies the description for this emulation packet.

4. Click **OK**.

5. On the **Choose Source** page, click **Select** in the Operation column of the specified detection source to enter the packet path detection page of the detection source. Click **Start** to start the detection. The system displays the detection flow in the flow chart and describes the detection process. The flow chart contains all modules the packets passes in the system. After the detection for a particular module is completed, the status indicator above the module indicates the detection results.

   - Green indicator() - Indicates the detection for this module has been passed. System will proceed with the detection. Hover your mouse over this step to view its introduction.

   - Yellow indicator() - Indicates the detection for this module has been passed, but there are potential security risks. System will proceed with the detection. Hover your mouse over this step to view its introduction and the detection results. You can click the **View Results** link to view the detailed detection report.

   - Red indicator() - Indicates the detection for this module fails to pass. System has stopped the detection. Hover your mouse over this step to view its introduction and the detection results. You can click the **View Results** link to view the detailed detection report. If the failure is caused by the policy rule configurations, you can click the link in the Policy Rule step to jump to the policy rule configuration page.

6. After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicator and detection result summary. You can click the **View Details** link to view the detailed detection report. The meanings of status indicators are as follows:

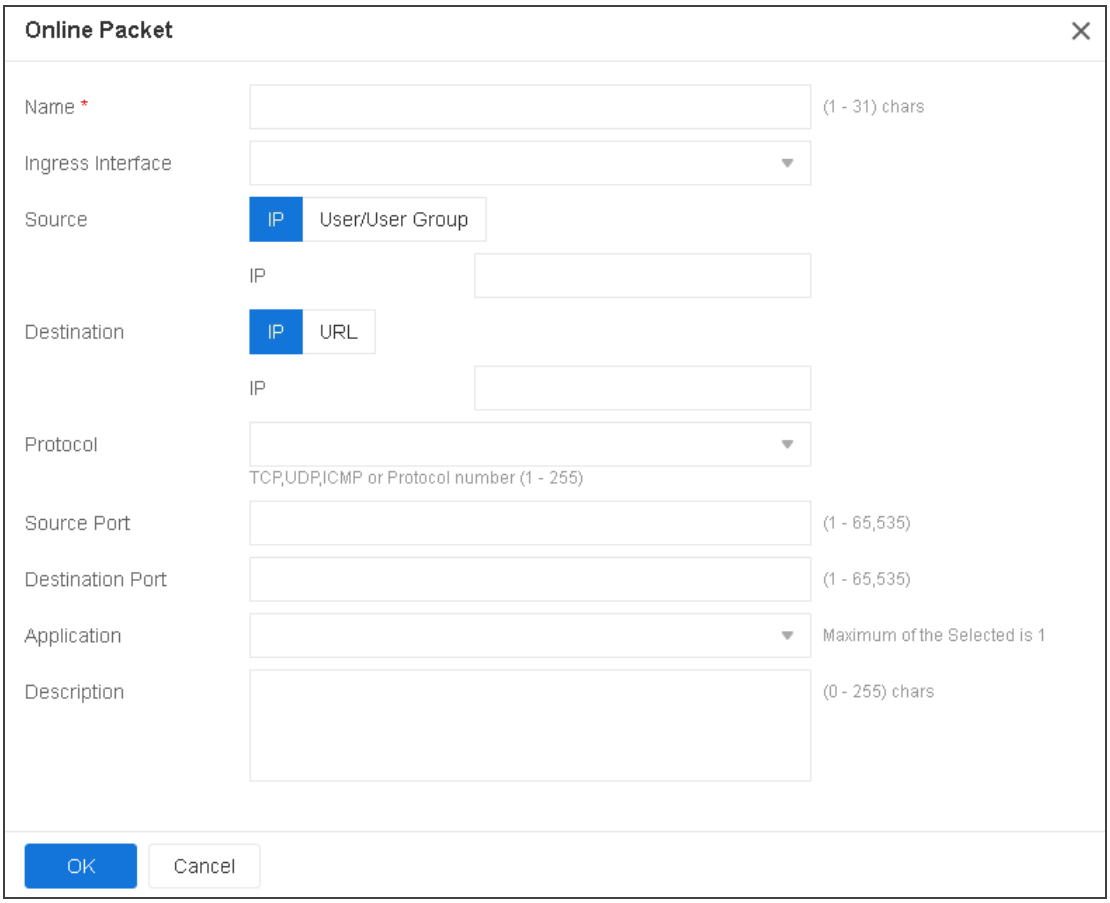
   - Green indicator() - Indicates the detected source has passed all detection.
   - Yellow indicator() - Indicates the detected source has passed all detection, but there are potential security risks in one or more steps. You can click the **View Details** link to view the potential risks and advice.
   - Red indicator() - Indicates not all detection is passed by the detected source. You can click the **View Details** link to view the failure reasons and advice.

Online Detection

To perform the online detection, take the following steps:

1. Select **System > Diagnostic Center > Packet Path Detection**.
2. Click **Choose Detected Source**.

3. Click **New** , in the drop-down list, select **Online Packet** tab.



Option	Description
Name	Specifies the name of the online packet.
Ingress Interface	Select the ingress interface of the online packet from the drop-down list.
Source	Specifies the source IP address or the user/user group of the online packet. • Address: Select the Address radio button and enter the IP address in the text box. • User/User Group: Select the User/User Group radio

Option	Description
	button and select the user/user group from the drop-down list.
Destination	Specifies the destination IP address of the online packet. • Address: Select the radio button and enter the IP address in the text box. • URL: Select the radio button and enter the URL in the text box.
Protocol	Specifies the protocol type or the protocol number of the packet.
Source Port	Specifies the source port of the online packet.
Destination Port	Specifies the destination port of the online packet.
Application	Specifies the application type of the online packet.
Description	Enter the description of the online packet in the text box.

4. Click **OK**.

5. On the **Choose Source** page, click **Select** in the Operation column of the specified detection source to enter the packet path detection page of the detection source. If needed, specify the detecting duration in the Detecting Duration section; Or select **Capture Packets** check box to enable the capture packets function.

6. Click **Start** to start the detection. The system displays the detection process. If errors occurr during the detection, a flow thumbnail in the area of the flow chart pops up to display the corresponding errors. After the detection is completed, you can click the flow thumbnail to

view the details. During each detection process, the system can pop up at most six thumbnails.

7. After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicator and detection result summary. You can click the **View Details** link to view the detailed detection report. About the meanings of status indicators, view step 3 in Emulation Detection.



Notes:

- If one of the following situations happens during the detection, the system will stop the detection.
  - Click the **Stop** button.
  - Reach the upper limit of the detecting duration. If you do not set the detecting duration, the detecting duration keeps the default value (30 minutes).
  - The total number of errors of the same type reaches 10. For example, the flow is blocked by the same policy.
  - The total number of errors of different types reaches 5. Errors of different types mean the errors occurred in different modules or errors occurred in one module but are different types.
  - After selecting the **Capture Packets** option, the size of the captured packet file reaches 10M during the detection.

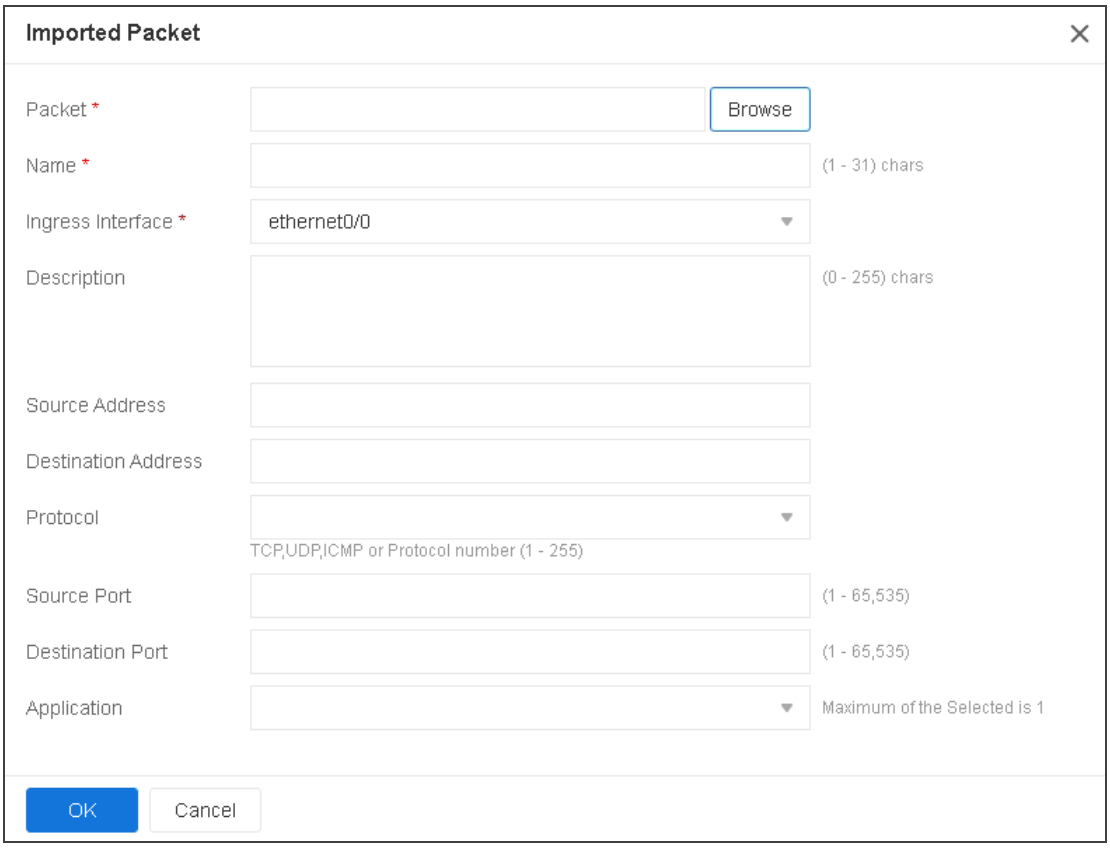
Imported Detection

To perform the imported detection, take the following steps:

1. Select **System > Diagnostic Center > Packet Path Detection**.

2. Click **Choose Detected Source**.

3. Click **New** , in the drop-down list, select **Imported Packet** tab.



Option	Description
Packet	Click the **Browse** button and select the packet file to import it. The maximum size of the imported packet file can be 20M. The format of packet can be .pcap or .pcapng.
Name	Specifies the name of the imported packet.
Ingress Interface	Select the ingress interface of the imported packet from the drop-down list.

Option	Description
Description	Enter the description of the online packet in the text box.
Source Address	Specifies the source IP address of the imported packet.
Destination Address	Specifies the destination IP address of the imported packet.
Protocol	Specifies the protocol type or the protocol number of the imported packet.
Source Port	Specifies the source port of the imported packet.
Destination Port	Specifies the destination port of the imported packet.
Application	Specifies the application type of the imported packet.

4. Click **OK**.

5. On the **Choose Source** page, click **Select** in the Operation column of the specified detection source to enter the packet path detection page of the detection source. Click **Start** to start the detection. The system displays the detection process in the Detection Process tab. If errors occurr during the detection, a flow thumbnail in the area of the flow chart pops up to display the corresponding errors. After the detection is completed, you can click the flow thumbnail to view the details. During each detection process, the system can pop up at most six thumbnails.

6. After the detection is completed, view the detection results in the Detection Result tab. The detection results include the status indicators and detection result summary. You can click the **View Details** link to view the detailed detection report. For the meanings of the status indicators, view step 3 in Emulation Detection.

Notes: If one of following situations happens during the detection, the system will stop the detection.

- Click the **Stop** button.
- The total number of errors of the same type reaches 10. For example the flow is blocked by the same policy.
- The total number of errors of different types reaches 5. Errors of different types mean the errors occurred in different modules or errors occurred in one module but are different types.
- The imported packets have been all detected.

Detected Sources

Click **Choose Detected Source** to display all existing detection sources in the system, including the emulation packet, online packet, and imported packet, on the **Choose Source** page. You can then perform the following actions:

- Click **Details** in the Result column to view the detection report of the detected source. On the report page, you can click **Download Packet** to export the detection packet to a local PC.
- Click **Export** in the Export Packet column to export the detected packet to the local PC.
- Click **Edit** in the Option column to edit the configurations of the detected source.
- Click **Delete** in the Option column to delete the detected source.

Packet Capture Tool

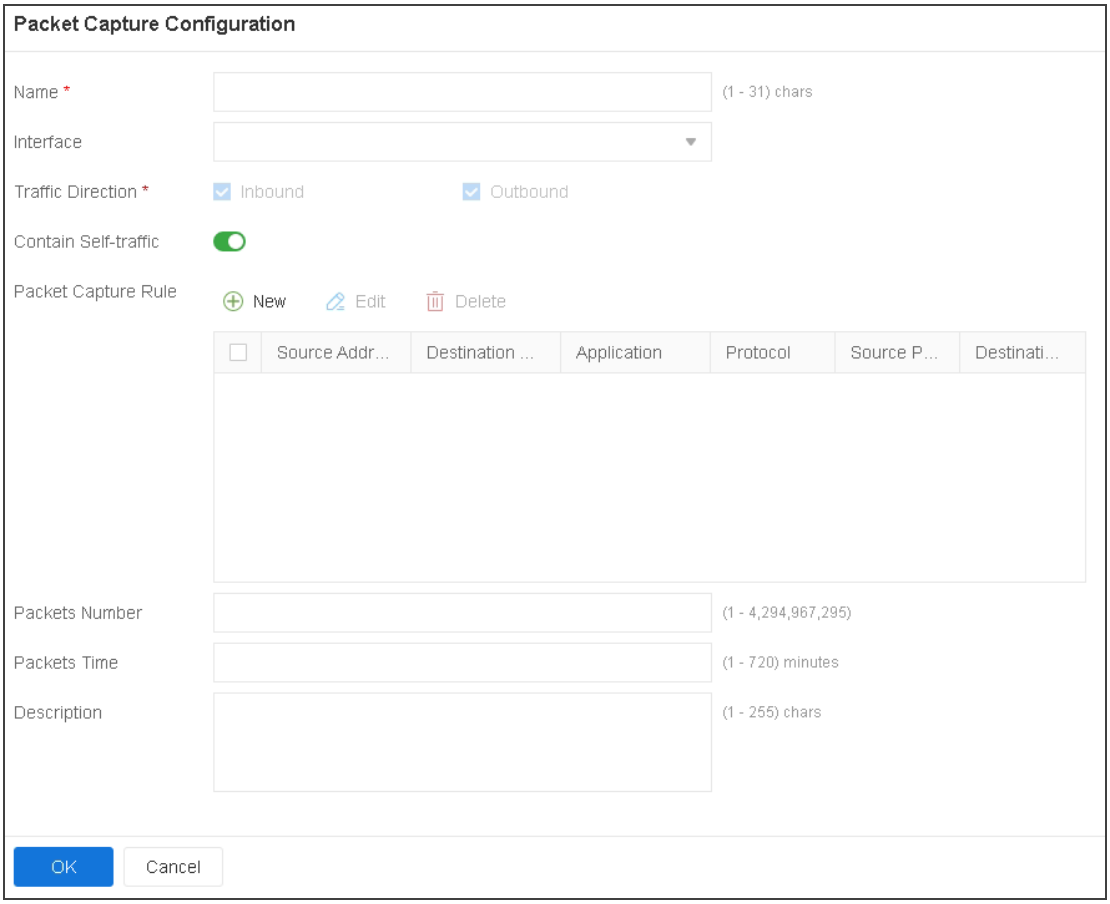
You can capture packets in the system with multiple capture tasks by Packets Capture Tools. You can set inbound and outbound traffic interfaces and add one or more packets capture rules to the task. This allows the system to capture packages with multiple conditions in real time. At the

same time, you can view the current captured and lost packages at any time. The captured packages can be downloaded or exported to a local location and then viewed through a third-party packet capture tool.

Configuring Packet Capture Tools

To capture packets, take the following steps:

1. Select **System > Diagnostic Center > Packet Capture Tool**.
2. Click **New**.

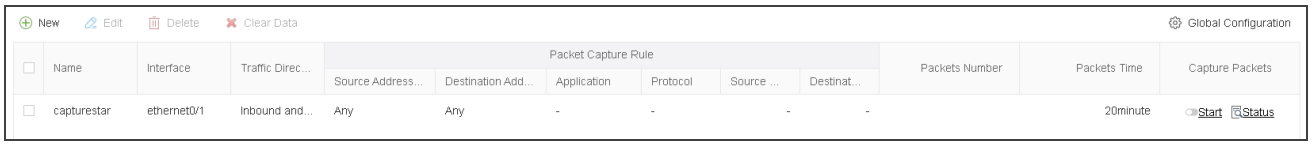


Option	Description
Name	Enter the name of the packets capture entry.
Interface	Select the interface used for the online packet capture task from

Option	Description
	the drop-down list.
Traffic Direction	Specifies the traffic direction of the interface. Valid values: Inbound and Outbound. By default, both Inbound and Outbound are selected. • Inbound: The online packet capture task captures packets of the inbound interface. If fails, the packets may be blocked by the firewall or not flow into the firewall. If no packets flow into the firewall, you can troubleshoot the upstream link or upstream device as needed. • Outbound: The online packet capture task captures packets of the outbound interface. If succeeds, you can troubleshoot the downstream link or downstream device as needed. • Inbound+Outbound: You can select both inbound and outbound and determine the actual traffic direction of the interface based on captured packets.
Contain Self-traffic	Turn on the switch to enable the Contain Self-traffic function. This way, captured packets contain traffic sent and received by the device itself. By default, this function is enabled.
Packet Capture Rule	Click **New**, and configure the packet capture rules in the **Packet Capture Rules** page. For the configuration method, refer to the Create a Packet Capture Rule. Select the check box of the packet capture rule in the list and

Option	Description
	click the **Edit** button to edit the configuration of the packet capture rule again. Select the check box of the packet capture rule in the list and click the **Delete** button to delete the packet capture rule.
Packets Number	Specifies the total number of packets that can be captured for the packet capture task. Valid values: 1 to 4294967295. During the effective period (packets time) of the packet capture task, if the number of packets captured reaches the configured number, the system automatically stops capturing packets.
Packets Time	Enter the packets time in the text box. The range is 1-720 minutes.
Description	Enter the entry description in the text box.

3. Click **OK**.



4. For each task, click **Start** button in the Capture Packets column to start capturing packets, and **Start** button will change to **Capturing**. Click the **Status** to view the current size/number of packets captured.

5. To stop capturing packets, click **Capturing** button in the Capture Packets column.

6. After you stop capturing packets or the capturing is completed, click **Download** at the top-right corner of the Capture Grid List to save the captured packets to a specified location.

7. You can select one or more file entries, and click **Export** at the top right corner of the list to export the package files. The exported grab package files are in compressed format.

8. To clear packet capture data, select a packet capture task and click the **Clear Data** button. All files captured under this task will be cleared.



Notes:

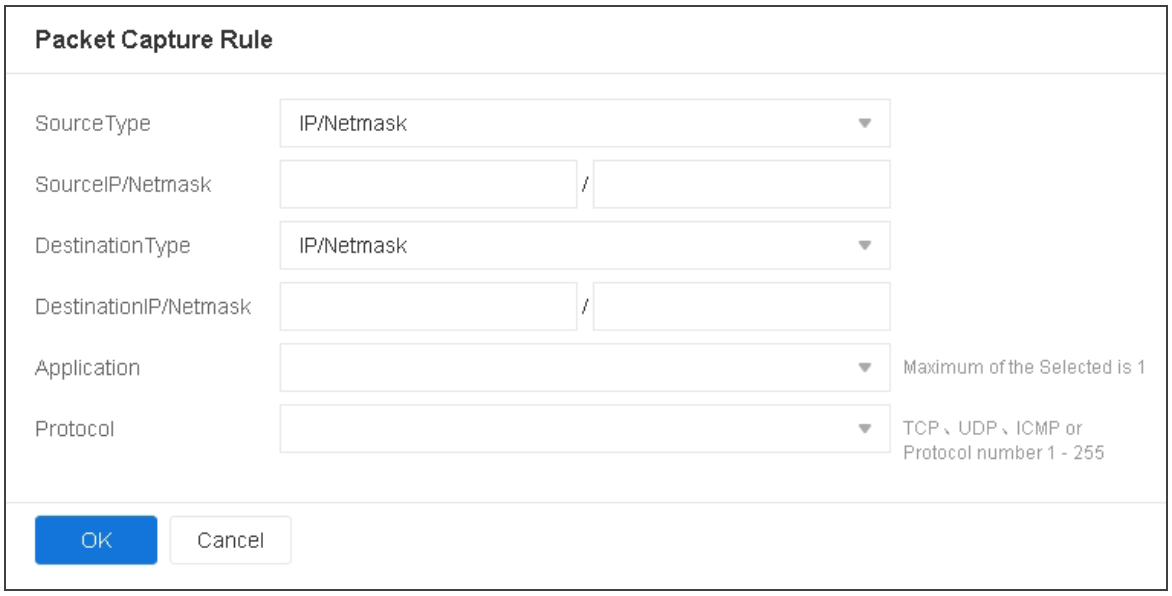
- At most 5 online packet capture tasks can be created.
- An online packet capture task cannot capture packets based on the tunnel interface and MGT0 interface.
- We recommend that the packet you capture at a time does not exceed 500 MB because a larger packet may fail to be exported caused by timeout.
- At most 5 packet capture tasks can be configured within each VSYS.
- You can start only one packet capture task within a single VSYS each time, and start a packet capture task within multiple VSYSes at the same time.
- When you delete a non-root VSYS, the packet capture tasks and packet capture files within the VSYS are deleted at the same time.

Create a Packet Capture Rule

To create a packet capture rule, take the following steps:

1. Select **System > Diagnostic Center > Packet Capture Tool**.
2. Click **New**.

3. Click **New** at **Package Capture Rule** to open the **Packet Capture Rule** page.



Option	Description
Source Type	Specify the source IP address/range or the user/user group of the packet. • IP/Netmask: Enter the IPv4 address and its mask in the text box. • IP Range: Enter the IPv4 range in the text box. • IPv6/Prefix: Enter the IPv6 address and its prefix in the text box. • IPv6 Range: Enter the IPv6 range in the text box. • User/User Group: Select the user/user group from the drop-down list.
Destination Type	Specify the destination IP address/range of the packet.

Option	Description
	• IP/Netmask: Enter the IPv4 address and its mask in the text box. • IP Range: Enter the IPv6 address and its range in the text box • IPv6/Prefix: Enter the IPv6 address and its prefix in the text box. • IPv6 Range: Enter the IPv6 range in the text box. • URL: Enter the URL in the text box.
Application	Specifies the application type of the packet. **Note**: Deprecated predefined applications cannot be added.
Protocol	Specifies the protocol type or the protocol number of the packet.
Source Port	When the protocol is TCP or UDP, the source port number can be specified. Specifies the source port of the packet.
Destination Port	When the protocol is TCP or UDP, the destination port number can be specified. Specifies the destination port of the packet.

4. Click **OK**.

Notes: A maximum of 8 packet capture rules can be created in the same packet capture task.

Packet Capture Global Configuration

The global configuration items of packet capture vary according to the type of device:

- For devices with hard disks, you can configure the percentage of the packet capture files to the total hard disk size only in the root VSYS.
- For devices without hard disks, in the root VSYS, you can configure the packet capture file save percent, the packet capture file save time, and the maximum memory usage; in the non-root VSYS, you can configure only the packet capture file save time.

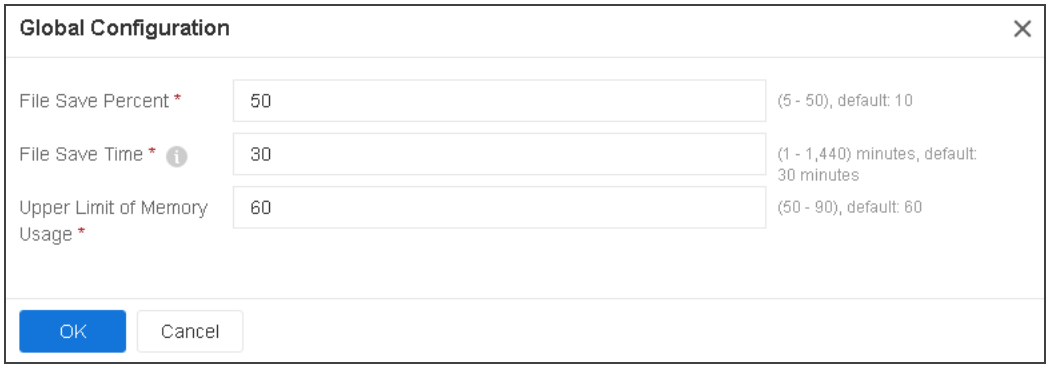
To configure the global configuration, take the following steps:

1. Select **System > Diagnostic Center > Packet Capture Tool**.
2. Click the **Global Configuration** button in the upper right corner of the page to open the **Global Configuration** page.
3. The global configuration page of the devices with hard disk is as follows:



Option	Description
Disk Space Percent	Enter the percentage of the packet capture file to the total hard disk size in the text box. The range is 5%-50%. The default value is 10%.

4. The global configuration page of packet capture for the devices without hard disk is as follows:



Option	Description
File Save Percent	Enter the maximum percentage of the remaining memory allowed by the packet capture file in the text box, the range is 5%-50%, and the default value is 10%. This option is available only in the root VSYS.
File Save Time	Enter the length of time the packet capture file is saved in the text box, the unit is minutes, the range is 1-1440 minutes, and the default value is 30 minutes.
Upper Limit Memory Usage	Enter the maximum percentage of memory that the packet capture file can use. Valid values: 50 to 90. Default value: 60. When the percentage of memory usage exceeds the upper limit, the system automatically stops capturing packets. This option is available only in the root VSYS.

5. Click **OK**.

Test Tools

DNS Query, Ping and Traceroute can be used when troubleshooting the network.

DNS Query

To check the DNS working status of the device, take the following steps:

1. Select **System** > **Diagnostic Center** > **Test Tools**.
2. Type a domain name into the **DNS Query** box.
3. Click **Test**, and the testing result will be displayed in the list below.

Ping

To check the network connecting status, take the following steps:

1. Select **System** > **Diagnostic Center** > **Test Tools**.
2. Type an IP address into the **Ping** box.
3. Click **Test**, and the testing result will be displayed in the list below.
4. The testing result contains two parts:
    - The Ping packet response. If there is no response from the target after timeout, it will print Destination Host Not Response, etc. Otherwise, the response contains sequence of packet, TTL and the response time.
    - Overall statistics, including number of packet sent, number of packet received, percentage of no response, the minimum, average and maximum response time.

Traceroute

Traceroute is used to test and record gateways the packet has traversed from the originating host to the destination. It is mainly used to check whether the network connection is reachable, and analyze the broken point of the network. The common Traceroute function is performed as follows: first, send a packet with TTL 1, so the first hop sends back an ICMP error message to indicate that this packet can not be sent (because of the TTL timeout); then this packet is re-sent, with TTL 2, TTL timeout is sent back again; repeat this process till the packet reaches the destination. In this way, each ICMP TTL timeout source address is recorded. As the result, the path from the originating host to the destination is identified. The system supports IPv4 and IPv6 peer addresses.

To test and record gateways the packet has traversed by Traceroute, take the following steps:

1. Select **System** > **Diagnostic Center** > **Test Tools**.
2. Select the VR in the Virtual Router drop-down list.
3. Select **IPv4** or **IPv6**.
4. Type an IP address into the **Traceroute** box.
5. Click **Test**, and the testing result will be displayed in the list below.

Debugging

Debugging is supported for you to check and analyze the problems.

Failure Feedback

To enable the failure feedback function:

1. Select **System** > **Device Management** > **Settings & Options**.
2. In the **System Settings** tab, turn on the switch next to **Failure Feedback**, and click OK. The system will automatically send the technical support file to the manufacturer.

System Debug Information

System debugging helps you to diagnose and identify system errors.

To export the system debugging information:

1. Select **System** > **System Debug**.
2. In the **System Options** tab, click **Export**. The system will package, save, and then export the "tech-support" file from the /etc/local/core directory.

Chapter 15 High Availability

HA, the abbreviation for High Availability, provides a fail-over solution for communications lines or device failure to ensure the smooth communication and effectively improve the reliability of the network.

To implement the HA function, you need to configure the two devices as HA clusters with identical settings for the following:

- Hardware platform
- Firmware version
- Virtual Router (enable VR simultaneously on two devices or not use VR on both devices)

When one device is not available or cannot handle the request from the client properly, the request will be promptly directed to the other device that works normally, thus ensuring uninterrupted network communication and greatly improving the reliability of communications.



Notes:

1. When configuring HA, the devices do not check the type or expiration date of the licenses. Instead, they compare whether the functions of the two HA devices are identical. That is, both devices need to have the same functions enabled or disabled simultaneously. As mentioned earlier, both HA devices need to be configured with the same VR features, which indicates that both devices have multi-VR enabled or both have it disabled.

2. The configuration of HA clusters is not affected if certain functions, such as AV, are not consistent on the two HA devices. In this scenario, the system sends an alarm showing that certain settings on the two devices are not consistent. It indicates that when the master device fails, the backup device



may have problems taking over its work. Settings that cause the above scenario include but are not limited to the below ones: enable or disable Antivirus/IPS/URL DB/Perimeter Traffic Filtering/Threat Prevention/Botnet C&C Prevention/Sandbox/IoT Monitor/VSYS, and install or not install Antivirus License/IPS License/URL DB License/PTF License/Threat Prevention License/Botnet Prevention License/IoT Monitor License/Twin-mode License/Cloud Sandbox Prevention License/Signature Database Application License/iQoS/VSYS License. It is suggested to concern on the alarms when the above functions are not consistent on the two HA devices.

3. We recommend that you set the engine ID of master device and backup device in the HA scenario to different values. This prevents that the trap host cannot receive trap alarms normally during HA switchover when the SNMPv3 trap function is enabled.

4. Do not configure the Local attribute on the business interface (interface carrying business traffic). Once configured, the interface will no longer participate in HA information synchronization. All configuration details, session information, and ARP entries associated with this interface will not be synchronized to the backup device, potentially leading to traffic disruption or abnormal network behavior, which could impact business operations. In addition, note that sub-interfaces and Virtual Forward interfaces automatically inherit the Local attribute of their parent interface. For example, if a physical interface is configured with the Local attribute, its sub-interfaces will also inherit this attribute. Therefore, special attention



needs to be paid to the Local attribute of the parent interface during configuration.

5. For configurations in some functional modules (policy (excluding aggregation policy), NAT, iQoS, ZTNA, DNS proxy, PBR routing, and ordered address book), if the order of configurations in the secondary device is not the same as that of the primary device, the system adjusts the order of configurations in the secondary device to be the same as that of the primary device when it performs batch synchronization.

6. No configuration changes are allowed on the primary and secondary devices until the batch synchronization is completed.

System supports two HA modes: Active-Passive (A/P) and Peer Active-Active (A/A).

- Active-Passive (A/P) mode: In the HA cluster, configure two devices to form an HA group, with one device acting as a primary device and the other acting as its backup device. The primary device is active, forwarding packets, and meanwhile synchronizes all of its network and configuration information and current session information to the backup device. When the primary device fails, the backup device will be promoted to primary and takes over its work to forward packets. This A/P mode is redundant, and features a simple network structure for you to maintain and manage.
- Peer Active-Active (A/A) mode: the Peer A/A mode is an HA Active-Active mode. In the Peer A/A mode, two devices are both active, perform their own tasks simultaneously, and monitor the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously. In the Peer A/A mode, only the device at the active status can send/receive packets. The device at the disabled status can make two devices have the same configuration information but its interfaces do not send/receive any packets. The Peer A/A mode is more flexible and is suitable for the deployment in the asymmetric routing environment.

Basic Concepts

HA Cluster

For the external network devices, an HA cluster is a single device which handles network traffic and provides security services. The HA cluster is identified by its cluster ID. After specifying an HA cluster ID for the device, the device will be in the HA state to implement HA function.

HA Group

System will select the primary and backup device of the same HA group ID in an HA cluster according to the HCMP protocol and the HA configuration. The primary device is in the active state and processes network traffic. When the primary device fails, the backup device will take over its work.

When assigning a cluster ID to the device, the HA group with ID 0 will be automatically created. In Active-Passive (A/P) mode, the device only has HA group 0.

HA Node

To distinguish the HA devices in an HA group, you can use the value of HA Node to mark the devices. StoneOS support the values of 0 and 1.

In the HA Peer mode, the system can decide which device is the master according to the HA Node value. In the HA group 0, the device whose HA Node value is 0 will be active and the device whose HA Node value is 1 is at the disabled status. In the HA group 1, this does not make sense because both times is HA Node value of 0

Virtual Forward Interface and MAC

In the HA environment, each HA group has an interface to forward traffic, which is known as the Virtual Forward Interface. The primary device of each HA group manages a virtual MAC (VMAC) address which is corresponding with its interface, and the traffic is forwarded on the interface. Different HA groups in an HA cluster cannot forward data among each other. VMAC address is defined by HA base MAC, HA cluster ID, HA group ID and the physical interface index.

HA Selection

In an HA cluster, if the group ID of the HA devices is the same, the one with higher priority will be selected as the primary device.

HA Synchronization

To ensure the backup device can take over the work of the primary device when it fails, the primary device will synchronize its information with the backup device. System supports two methods to synchronize: real-time synchronization and batch synchronization. When the primary device has just been selected successfully, the batch synchronization will be used to synchronize all information of the primary device to the backup device. When the configurations change, the real-time synchronization will be used to synchronize the changed information to the backup device. Except for the HA related configurations and local configurations (for example, the host name), all the other configurations will be synchronized.

There are three types of information that can be synchronized: configuration information, files and RDO (Runtime Dynamic Object). The specific content of RDO includes:

- Session information (The following types of session information will not be synchronized: the session to the device itself, tunnel session, deny session, ICMP session, and the tentative session)
- IPsec VPN information
- SSL VPN information
- DNS cache mappings
- ARP table
- PKI information
- DHCP information

- MAC table
- WebAuth information

Configuring HA Active-Passive (A/P) Mode

This feature may vary slightly on different platforms, if there is a conflict between this guide and the actual page, the latter shall prevail.

The main configuration steps of the HA Active-Passive (A/P) mode include:

1. Configure an HA Virtual Forward Interface. For more information on configuring the interface, see "Configuring an Interface" on Page 158.
2. Configure the HA working mode as Active-Passive.
3. Configure the HA link, including an HA link interface and an HA link IP address, for the device synchronization and HA packets transmission.
4. Configure an HA cluster. Specify the HA cluster ID and HA node ID to enable the HA function.
5. Configure an HA group. Specify the priority for devices (for selecting the master) and HA messages parameters.

To configure HA Active-Passive (A/P) mode, take the following steps:

1. Go to **System > HA**.
2. Select the HA working mode as Active-Passive, which means that one device in the HA cluster works in active mode and the other works in backup mode.
   Configure HA Active-Passive (A/P) mode.

Option	Description
Control link interface 1	Specifies the name of the HA control link interface 1. The control link interface is used to synchronize all data between two devices.
Control link	Specifies the name of HA control link interface 2 (Backup

Option	Description
interface 2	interface). **Note**: You can specify at most one aggregate interface as the HA control link interface, or at most two physical interfaces as the HA control link interface.
Assist link interface	Specifies the name of the HA assist link interface to receive and send heartbeat packets (Hello packets) and ensure the main and backup device of HA switches normally when the HA link fails. **Notes**: • Before the HA link is restored, the HA assist link interface can only receive and send heartbeat packets and the data packets cannot be synchronized. You are advised not to modify the current configurations. After the HA link is restored, manually synchronize session information. • The HA assist link interface must use an interface other than the HA link interface and be bound to the zone. • You need to specify the same interface as the HA assist link interface for the main and backup device, and ensure that the interface of the main and backup device belongs to the same VLAN.
Data link interface 1	Specifies the name of the HA data link interface 1. The data link interface is used to synchronize the data packet information, such as session information. After specifying this data link, the session information will be synchronized over this

Option	Description
	data link. You can configure the physical interface or aggregate interface as the interface of the data link.
Data link interface 2	Specifies the name of the HA data link interface 2 (backup interface). Notes: • You can specify at most one aggregate interface as the HA data link interface, or at most two physical interfaces as the HA data link interface. • When both the control link interface and data link interface are configured, you are advised to configure the data link interface as being an aggregate interface to prevent session synchronization failures at a data link failure.
IP Type	Specifies the IP address type of the HA link. This option is available only when the device's IP version is IPv6.
IP Address/IPv6 Address	Specifies the IP address of the HA link, which is used to synchronize all data between two devices and transmit HA packets. • When the IP address type is IPv4 or the device's IP version is IPv4, specifies the IPv4 address and netmask of the HA link interface, in format A.B.C.D/M. The value of M can be an integer ranging from 1 to 32 or a string in dotted decimal notation. • When the IP address type is IPv6, specifies the IPv6

Option	Description
	address and prefix length of the HA link interface, in format X.X.X.X::X/M. X.X.X.X::X is the IPv6 address prefix. M is the prefix length. The value range of the prefix length is 1 to 128.
HA Virtual MAC	Specifies the virtual MAC address of the HA device interface: • Default: Use the system default generated HA dummy MAC address generated by the system. • HA base virtual MAC: Specifies the HA base virtual MAC address. To ensure unique system-generated HA virtual MAC addresses and simplify future maintenance, you can assign specific HA virtual MAC addresses by specifying HA base virtual MAC. It is recommended that you use the system-recommended HA base virtual MAC. No device reboot is required for the configuration to take effect. Note: • HA base virtual MAC function is supported only in HA A/P mode and needs to be configured before the HA function is enabled. • 0x00000000, 0x0000000, 0xFFFFFFFF, 0xFFFFFFF or multicast addresses (i.e., the second hexadecimal number is odd) are invalid. • IF the HA function enabled and you want to modify the

Option	Description
	HA virtual MAC prefix or HA base virtual MAC, you may need to disable the HA function first.
HA cluster ID	Specifies an ID for HA cluster. Saving the configuration of an HA cluster ID will enable the HA function. Deleting the configuration of it will disable the HA function. The value ranges from 1~8.
Node ID	Specify the node ID. The two devices should be configured with different node IDs. The value range is 0 to 1. Certain devices support automatic negotiation of the node ID. It is recommended to manually configure the node ID.
HA Negotiation Mode	Specifies the HA negotiation mode. Valid values: Default, Same Network Segment. • Default: indicates that devices in the same network segment use multicast communication for HA negotiation. This is the default option. • Same Network Segment: indicates that devices in the same network segment use layer-2 unicast communication for HA negotiation. After you select this option, you need to configure the HA peer IP address, or configure both the HA peer IP address and MAC address.
HA Peer IP/HA Peer	Specifies the IP address of the peer device, which is used to synchronize all data between two devices and transmit HA

Option	Description
IPv6	packets. • When the IP address type of HA link is IPv4 or the device's IP version is IPv4, enter the IPv4 address of HA peer device. • When the IP address type of HA link is IPv6, enter the IPv6 address of HA peer device.
HA Peer MAC	Enter the MAC address of HA peer device, i.e. the MAC address of the heartbeat interface.
MTU	Specifies the MTU value of HA link interface. If the size of the message exceeds the MTU value of the HA link interface, the sender will fragment and send the message and the receiver will reassemble the fragments. Valid values: 1280 to 1600. Unit: bytes. Default value: 1500.
L3 port down-up	If this function is disabled, the following types of physical interfaces do not perform down-up operations when the device is switched from a master device to a backup device for HA switchover: • The physical interface that is bound to a Layer 3 zone. • The physical interface that belongs to a redundant interface, and the redundant interface is bound to a Layer 3 zone. • The physical interface that belongs to an aggregate interface, and the aggregate interface is bound to a Layer 3

Option	Description
	zone.
HA group configuration	HA group configuration consists of the following items: • Group: After you specify the HA working mode, the group ID is automatically generated and cannot be changed. In A/P mode, only Group 0 is available. • Priority: Specifies the priority of the current device in the HA group. The device with the highest priority (the lowest value) is elected as the primary device. Valid values: 1 to 254. • Preempt: Specifies whether to enable the preempt mode and the preempt time. If you enable this mode, the device will upgrade itself to the primary device once its priority is higher than the current primary device, and the current primary device becomes a secondary device. If you enter a value of 0, it indicates that you disable the preempt mode. In this case, the device can only substitute the primary device in case of primary device failure even if the priority of the device is higher than that of the primary device. Valid values: 0 to 600. Unit: seconds. • Hello interval: Specifies the Hello interval value. The Hello interval indicates the interval for the HA device to send heartbeats (Hello packets) to other devices in the

Option	Description
	HA group. The Hello interval in the same HA group must be identical. Valid values: 50 to 10000. Unit: milliseconds. • Hello threshold: Specifies the threshold value of the Hello message. If the device does not receive the specified number of Hello messages from the other device, it will suppose the other device's heartbeat stops. Valid values: 3 to 255. • Gratuitous ARP packet number: Specifies the number of gratuitous ARP packets. When the backup device is elected as the primary device, it will send an ARP request packet to the network to inform the relevant network devices to update its ARP table. Valid values: 10 to 180. • Track Object: Specifies the track object you have configured or click ⊕ to create a track object. The track object is used to monitor the working status of the device. Once finding the device stop working normally, system will take the corresponding action. • Description: Specifies the description of the HA group.
Auto-check for Configuration Consistency of Master and	Enable this function to automatically check whether configurations between the master and the backup devices are the same. After this function is enabled, the system will perform one check immediately and afterward at the interval of 1 hour.

Option	Description
Backup	After every check, the system will refresh the Latest Check Result option. If a configuration inconsistency is found, a log will be also recorded. To view inconsistency details, you can perform a check again via the Manual Check for Consistency of Master and Backup option. This function is disabled by default. **Note**: Please enable the "Auto-check for Configuration Consistency of Master and Backup" function on the master device after the HA negotiation is successful. When this function is enabled, the backup device synchronizes the configuration.
Manual Check for Consistency of Master and Backup	Click **Query** to perform one-time configuration consistency check between the master and the backup devices. After the check is finished, the Latest Check Result option will be automatically refreshed. If different configurations exist, a page showing detailed configuration differences will be prompted. **Notes**: • On devices supporting the VSYS function and loaded with the VSYS license, click **Details** to view the details for each VSYS. In other conditions, the details are directly displayed. • Please perform one-time configuration consistency check on the master device after the HA negotiation is successful.
Latest Check Result	Displays the configuration consistency check result, check time and query type.

3. Click **OK.**

HA Interface Traffic Monitor

The HA interface traffic monitor function statistically analyzes the historical traffic trend of HA interfaces in a specified statistical period.

To view the historical traffic trend of HA interfaces, go to **System > HA**, and then click the HA Interface Traffic Monitor button.

- Select a different Statistical Period from the drop-down menu to view the statistical information in that period of time.
- Click and to switch between the curve chart and the area chart.
- Click " " to refresh the monitoring data.
- Click " " to collapse the chart or click " " to expand the chart.
- Hover your mouse over the chart to view upstream traffic, downstream traffic or total traffic of the HA interface.
- Click **Upstream Traffic**, **Downstream Traffic** or **Total Traffic**, system displays the interface traffic of the specified object.

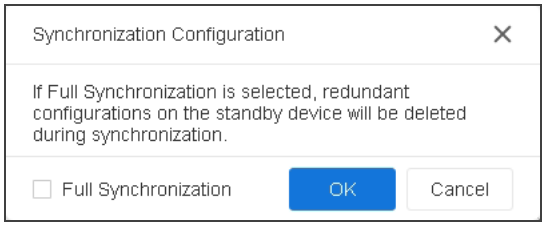
HA Manual Synchronization

As described in HA synchronization, the system uses batch synchronization to synchronize all the master device information to the backup device when the HA master device election is successful. However, in some cases, the master and backup configuration information may not be synchronized. For example, the configuration order in the backup device is not consistent with that of the master device, there are configurations in the backup device that are not included in the master device, or the configuration of the backup device reaches the capacity limit, resulting in the loss of the configurations that have been synchronized from the master device. In this case,

you need to manually perform batch synchronization to synchronize the configuration information of the master and backup devices. When manually synchronizing the configuration, you can further configure the full synchronization function. This function can delete the configuration information of the backup device that is more than that of the master device while batch synchronizing the configuration of the master device, and adjust the configuration order of the backup device to ensure that the configuration information and configuration order of the master and backup devices are consistent.

To manually synchronize configurations, take the following steps:

1. Select **System** > **HA**.
2. Click **HA Synchronize Configuration**. In the **Synchronization Configuration** dialog box, you can select **Full Synchronization**. In this case, if there are configurations in the backup device that are not in the master device, these additional configurations will be removed during the synchronization of master device configuration information. If you do not select **Full Synchronization**, only the configuration information of the master device is synchronized. By default, the Full Synchronization function is not enabled.



3. Click **OK**.

Notes:

- Only the master device supports the HA manual synchronization function.
- For some functional modules (policy (without aggregation policy), NAT, iQoS, ZTNA, DNS proxy, PBR routing, ISP routing, static routing, interface,

address book, and service book), the redundant configurations in the backup device can be deleted only if they belong to one of the above functional modules.

- When deleting a configuration that the backup device has more than the master device, if the configuration has been referenced by other function modules, it cannot be deleted and needs to be un-referenced before it can be deleted.

HA Session Synchronization

By default, information about sessions between HA devices are automatically synchronized. This process generates additional traffics, which may compromise the performance when the device is overloaded. You can use the **ha sync rdo session disable** command to disable the automatic synchronization function of HA sessions based on device loads. This ensures device stability.

To manually synchronize HA sessions after the automatic synchronization function of HA sessions is disabled, select **System** > **HA**. On the **HA** page, click **HA Synchronize Session**.

HA Primary/Secondary Switchover

To manually performs primary/secondary switchover, select **System** > **HA**. On the **HA** page, click **HA Master Switch Over**.

Viewing the HA Status of the Device

In the HA environment, you can view the HA status of current device at the **Device Name** in the upper right corner of the main page of system.



- M: **M** state that represents the current device is the master.
- B: **B** state that represents the current device is the backup.

Configuring HA Peer Active-Active (A/A) Mode

This feature may vary slightly on different platforms, if there is a conflict between this guide and the actual page, the latter shall prevail.

The main configuration steps of the HA Peer Active-Active (A/A) mode include:

1. Configure an HA Virtual Forward Interface. For more information on configuring the interface, see "Configuring an Interface" on Page 158.
2. Configure the HA working mode as Peer Active-Active.
3. Configure the HA link, including an HA link interface and an HA link IP address, for the device synchronization and HA packets transmission.
4. Configure an HA cluster. Specify the HA cluster ID and HA node ID to enable the HA function.
5. Enable the HA peer mode.
6. Configure an HA group. Specify the priority for devices (for selecting the master) and HA messages parameters.

To configure HA Peer Active-Active (A/A) mode, take the following steps

1. Go to **System > HA**.
2. Select the HA working mode as Peer Active-Active, which means that both devices in the HA cluster work in active mode.
   Configure HA Peer Active-Active (A/A) mode.

Option	Description
Control link interface 1	Specifies the name of the HA control link interface 1. The control link interface is used to synchronize all data between two devices.

Option	Description
Control link interface 2	Specifies the name of HA control link interface 2 (Backup interface). **Note**: You can specify at most one aggregate interface as the HA control link interface, or at most two physical interfaces as the HA control link interface.
Assist link interface	Specifies the name of the HA assist link interface to receive and send heartbeat packets (Hello packets) and ensure the main and backup device of HA switches normally when the HA link fails. **Notes**: • Before the HA link is restored, the HA assist link interface can only receive and send heartbeat packets and the data packets cannot be synchronized. You are advised not to modify the current configurations. After the HA link is restored, manually synchronize session information. • The HA assist link interface must use an interface other than the HA link interface and be bound to the zone. • You need to specify the same interface as the HA assist link interface for the main and backup device, and ensure that the interface of the main and backup device belongs to the same VLAN.
Data link interface 1	Specifies the name of the HA data link interface 1. The data link interface is used to synchronize the data packet inform-

Option	Description
	ation, such as session information. After specifying this data link, the session information will be synchronized over this data link. You can configure the physical interface or aggregate interface as the interface of the data link.
Data link interface 2	Specifies the name of the HA data link interface 2 (backup interface). Notes: • You can specify at most one aggregate interface as the HA data link interface, or at most two physical interfaces as the HA data link interface. • When both the control link interface and data link interface are configured, you are advised to configure the data link interface as being an aggregate interface to prevent session synchronization failures at a data link failure.
IP Type	Specifies the IP address type of the HA link. This option is available only when the device's IP version is IPv6.
IP Address/IPv6 Address	Specifies the IP address of the HA link, which is used to synchronize all data between two devices and transmit HA packets. • When the IP address type is IPv4 or the device's IP version is IPv4, specifies the IPv4 address and netmask of the HA link interface, in format A.B.C.D/M. The value of M can be an integer ranging from 1 to 32 or a string in

Option	Description
	dotted decimal notation. • When the IP address type is IPv6, specifies the IPv6 address and prefix length of the HA link interface, in format X.X.X.X::X/M. X.X.X.X::X is the IPv6 address prefix. M is the prefix length. The value range of the prefix length is 1 to 128.
HA cluster ID	Specifies an ID for HA cluster. Saving the configuration of an HA cluster ID will enable the HA function. Deleting the configuration of it will disable the HA function. The value ranges from 1~8.
Node ID	Specify the node ID. The two devices should be configured with different node IDs. The value range is 0 to 1. Certain devices support automatic negotiation of the node ID. It is recommended to manually configure the node ID.
Peer-mode	Click to enable the HA peer mode. By default, the group 0 in the device whose HA Node ID is 0 will be active and the group 0 in the device whose HA Node ID is 1 will be in the disabled status. The group 1 in the device whose HA Node ID is 1 will be active and the group 1 in the device whose HA Node ID is 0 will be in the disabled status.
Symmetric-routing	Enable this function to make the device work in the symmetrical routing environment. It is recommended to enable this function when the inbound and outbound packets of a ses-

Option	Description
	sion are processed on the same device. When enabled, the system will simplify the session processing process. This function is disabled by default, that is, the device works in asymmetric routing mode by default.
HA Negotiation Mode	Specifies the HA negotiation mode. Valid values: Default, Same Network Segment. • Default: indicates that devices in the same network segment use multicast communication for HA negotiation. This is the default option. • Same Network Segment: indicates that devices in the same network segment use layer-2 unicast communication for HA negotiation. After you select this option, you need to configure the HA peer IP address, or configure both the HA peer IP address and MAC address.
HA Peer IP/HA Peer IPv6	Specifies the IP address of the peer device, which is used to synchronize all data between two devices and transmit HA packets. • When the IP address type of HA link is IPv4 or the device's IP version is IPv4, enter the IPv4 address of HA peer device. • When the IP address type of HA link is IPv6, enter the IPv6 address of HA peer device.

Option	Description
HA Peer MAC	Enter the MAC address of HA peer device, i.e. the MAC address of the heartbeat interface.
MTU	Specifies the MTU value of HA link interface. If the size of the message exceeds the MTU value of the HA link interface, the sender will fragment and send the message and the receiver will reassemble the fragments. Valid values: 1280 to 1600. Unit: bytes. Default value: 1500.
L3 port down-up	If this function is disabled, the following types of physical interfaces do not perform down-up operations when the device is switched from a master device to a backup device for HA switchover: • The physical interface that is bound to a Layer 3 zone. • The physical interface that belongs to a redundant interface, and the redundant interface is bound to a Layer 3 zone. • The physical interface that belongs to an aggregate interface, and the aggregate interface is bound to a Layer 3 zone.
HA group configuration	HA group configuration consists of the following items: • Group: After you specify the HA working mode, the group ID is automatically generated and cannot be changed. In peer A/A mode, both Group 0 and Group 1 are available.

Option	Description
	• Priority: Specifies the priority of the current device in the HA group. The device with the highest priority (the lowest value) is elected as the primary device. Valid values: 1 to 254. • Preempt: Specifies whether to enable the preempt mode and the preempt time. If you enable this mode, the device will upgrade itself to the primary device once its priority is higher than the current primary device, and the current primary device becomes a secondary device. If you enter a value of 0, it indicates that you disable the preempt mode. In this case, the device can only substitute the primary device in case of primary device failure even if the priority of the device is higher than that of the primary device. Valid values: 0 to 600. Unit: seconds. • Hello interval: Specifies the Hello interval value. The Hello interval indicates the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. Valid values: 50 to 10000. Unit: milliseconds. • Hello threshold: Specifies the threshold value of the Hello message. If the device does not receive the specified number of Hello messages from the other device,

Option	Description
	it will suppose the other device's heartbeat stops. Valid values: 3 to 255. • Gratuitous ARP packet number: Specifies the number of gratuitous ARP packets. When the backup device is elected as the primary device, it will send an ARP request packet to the network to inform the relevant network devices to update its ARP table. Valid values: 10 to 180. • >Track Object: Specifies the track object you have configured or click  to create a track object. The track object is used to monitor the working status of the device. Once finding the device stop working normally, system will take the corresponding action. • Description: Specifies the description of the HA group.
Auto-check for Configuration Consistency of Master and Backup	Enable this function to automatically check whether configurations between the master and the backup devices are the same. After this function is enabled, the system will perform one check immediately and afterward at the interval of 1 hour. After every check, the system will refresh the Latest Check Result option. If a configuration inconsistency is found, a log will be also recorded. To view inconsistency details, you can perform a check again via the Manual Check for Consistency of Master and Backup option. This function is disabled by default. **Note**: Please enable the "Auto-check for Configuration Con-

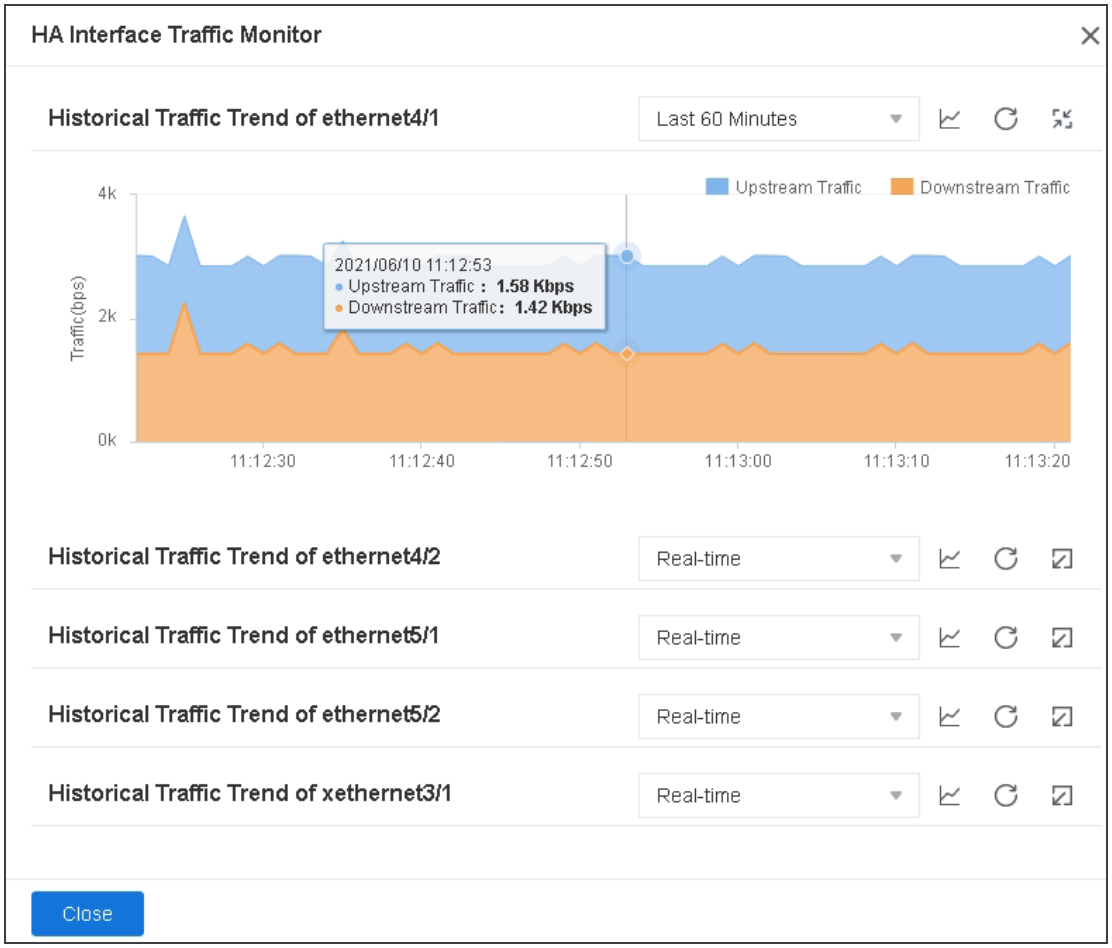
Option	Description
	sistency of Master and Backup" function on the master device after the HA negotiation is successful. When this function is enabled, the backup device synchronizes the configuration.
Manual Check for Consistency of Master and Backup	Click **Query** to perform one-time configuration consistency check between the master and the backup devices. After the check is finished, the Latest Check Result option will be automatically refreshed. If different configurations exist, a page showing detailed configuration differences will be prompted. **Notes**: • On devices supporting the VSYS function and loaded with the VSYS license, click **Details** to view the details for each VSYS. In other conditions, the details are directly displayed. • Please perform one-time configuration consistency check on the master device after the HA negotiation is successful.
Latest Check Result	Displays the configuration consistency check result, check time and query type.

3. Click **OK**.

HA Interface Traffic Monitor

The HA interface traffic monitor function statistically analyzes the historical traffic trend of HA interfaces in a specified statistical period.

To view the historical traffic trend of HA interfaces, go to **System > HA**, and then click the HA Interface Traffic Monitor button.



- Select a different Statistical Period from the drop-down menu to view the statistical information in that period of time.
- Click and to switch between the curve chart and the area chart.
- Click " " to refresh the monitoring data.
- Click " " to collapse the chart or click " " to expand the chart.
- Hover your mouse over the chart to view upstream traffic, downstream traffic or total traffic of the HA interface.

- Click **Upstream Traffic**, **Downstream Traffic** or **Total Traffic**, system displays the interface traffic of the specified object.

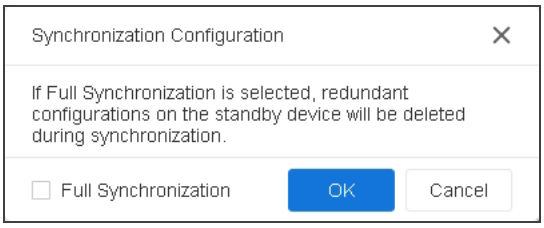
HA Manual Synchronization

As described in HA synchronization, the system uses batch synchronization to synchronize all the master device information to the backup device when the HA master device election is successful. However, in some cases, the master and backup configuration information may not be synchronized. For example, the configuration order in the backup device is not consistent with that of the master device, there are configurations in the backup device that are not included in the master device, or the configuration of the backup device reaches the capacity limit, resulting in the loss of the configurations that have been synchronized from the master device. In this case, you need to manually perform batch synchronization to synchronize the configuration information of the master and backup devices. When manually synchronizing the configuration, you can further configure the full synchronization function. This function can delete the configuration information of the backup device that is more than that of the master device while batch synchronizing the configuration of the master device, and adjust the configuration order of the backup device to ensure that the configuration information and configuration order of the master and backup devices are consistent.

To manually synchronize configurations, take the following steps:

1. Select **System** > **HA**.
2. Click **HA Synchronize Configuration**. In the **Synchronization Configuration** dialog box, you can select **Full Synchronization**. In this case, if there are configurations in the backup device that are not in the master device, these additional configurations will be removed during the synchronization of master device configuration information. If you do not select **Full Synchronization**, only the configuration information of the master device is synchronized. By

default, the Full Synchronization function is not enabled.



3. Click **OK**.

Notes:

- Only the master device supports the HA manual synchronization function.
- For some functional modules (policy (without aggregation policy), NAT, iQoS, ZTNA, DNS proxy, PBR routing, ISP routing, static routing, interface, address book, and service book), the redundant configurations in the backup device can be deleted only if they belong to one of the above functional modules.
- When deleting a configuration that the backup device has more than the master device, if the configuration has been referenced by other function modules, it cannot be deleted and needs to be un-referenced before it can be deleted.

HA Session Synchronization

By default, information about sessions between HA devices are automatically synchronized. This process generates additional traffics, which may compromise the performance when the device is overloaded. You can use the **ha sync rdo session disable** command to disable the automatic synchronization function of HA sessions based on device loads. This ensures device stability.

To manually synchronize HA sessions after the automatic synchronization function of HA sessions is disabled, select **System** > **HA**. On the **HA** page, click **HA Synchronize Session**.

HA Primary/Secondary Switchover

To manually performs primary/secondary switchover, select **System** > **HA**. On the **HA** page, click **HA Master Switch Over**.

Viewing the HA Status of the Device

In the HA environment, you can view the HA status of current device at the **Device Name** in the upper right corner of the main page of system.



- M: **M** state that represents the current device is the master.
- B: **B** state that represents the current device is the backup.

Chapter 16 System Management

The device's maintenance and management include:

- " System Information" on Page 1685
- "Device Management" on Page 1690
- "Configuration File Management" on Page 1734
- "Warning Page Management" on Page 1745
- "SNMP" on Page 1750
- "Upgrading System" on Page 1786
- "License" on Page 1796
- "Mail Server" on Page 1812
- "SMS Parameters" on Page 1828
- "Extended Services" on Page 1765
- "Test Tools" on Page 1650
- "VSYS (Virtual System)" on Page 1828
- "The Maximum Concurrent Sessions" on Page 1847
- "Password-free Login to CLI via WebUI" on Page 1689

System Information

Users can view the general information of the system in the System Information page, including Serial Number, Hostname, Platform, System Time, System Uptime, HA State, Firmware, Boot File, Signature Database and so on.

Viewing System Information

To view system information, select **System** > **System and Signature Database**.

System Information	
Serial Number	Show the serial number of device.
Hostname	Show the name of device.
Platform	Show the platform model of device.
Product Category	Show the category name of the product. Click button, in the <Configure> Page, enter a user-defined product name with a range of 0-128 characters in the product category text box. Click **OK** button. After modification, the login page will display the customized product name.
System Time	Show the system date and time of device.
System Uptime	Show the system uptime of device.
HA State	Show the HA status of device. • Standalone: Non-HA mode that represents HA is disabled. • Init: Initial state. • Hello: Negotiation state that represents the device is consulting the relationship between the master and backup. • Master: Master state that represents the current device is the master. • Backup: Backup state that represents the current device is the backup. • Failed: Fault state that represents the device has failed.

System Information	
	• Disabled: Disabled state which represents the interface is disabled. Only Peer Active-Active mode has this state.
Firmware	Show the current firmware version of the device.
Boot File	Show the version name of the current device boot file and the time when the file was compiled.
API	Get RESTful API User Guide.
Signature DB Information	
Check Immediately	Click the **Check Immediately** to update and display the latest version number of the signature library. Note: The signature database license should been activated and the system already has a signature library version.
Application Identification Signature	Show the current version of the application signature database and the date of the last update.
URL Category Signature	Show the current version of the URL signature database and the date of the last update.
Encrypted Traffic Detection Library	Show the current version of the encrypted traffic detection library and the date of the last update.
IP Reputation Database	Show the current version of the perimeter traffic filtering signature database and the date of the last update.
Anti-Virus Signature	Show the current version of the antivirus signature database and the date of the last update.
Anti-Virus Intel-	Show the current version of the antivirus intelligence file engine data-

System Information	
ligence File Engine Database	base and the date of the last update. Note: Devices except SG-6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800, and SG-6000-A2200 support the function.
IPS Signature	Show the current version of the IPS signature database and the date of the last update.
Botnet Prevention Signature	Show the current version of the Botnet Prevention signature database and the date of the last update.
SSL Proxy Domain White List Signature Database	Displays the current version of the SSL proxy domain whitelist signature database and the release date of the current version.
Sandbox Whitelist DB	Show the current version of the Sandbox Whitelist DB and the date of the last update.
ISP Information Database	Show the current version, release date, and latest version of the ISP information database.
IP Geography Database	Show the current version, release date, and latest version of the IP geography database.
Share Access Signature Database	Show the current version, release date, and latest version of the share access signature database.
Trusted Root Certificate	Show the current version, release date, and latest version of the trusted root certificate.
MITRE	Show the current version, release date, and latest version of the

System Information	
ATT&CK® Knowledge Base	MITRE ATT&CK® knowledge base.

Notes: Except Encrypted traffic detection database,SSL proxy domain whitelist signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database, only when the license of a signature database is installed can the system displays the information about this signature database. To install a signature database license, see License.

Password-free Login to CLI via WebUI

To improve the convenience of O&M on devices, the system supports the function of password-free login to the CLI via WebUI. After you log in to the device via WebUI, you can click the CLI icon in the upper-right corner. In the command window that appears, you can directly configure the device by using commands without the need to enter the username and password.



Notes: When you use the function:

- We recommend that you use Microsoft Edge or Chrome 45 and later to access the WebUI of the device.
- The management port of the device (some devices have a default MGT port), trusted host, and administrator need to enable the HTTP or HTTPS services.
- If the user is an administrator with a customized administrator role, it is necessary to enable CLI privileges for that administrator role. To enable CLI privileges for an administrator role, please refer to "Admin Roles" on Page 1701.



- Logging in or out of the CLI generates corresponding event logs.
- You can use the **webconsole max-clients** *number* command to configure the maximum number of connections for the CLI window, which indicates the maximum number of CLI windows that can be opened simultaneously on the same device.

Device Management

Introduces how to configure the Administrator, Trust Host, MGT Interface, System Time, NTP Key and system options.

- **Administrators**: Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles.
- **Admin Roles**: Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles. The pre-defined administrator role cannot be deleted or edited. You can customize administrator roles according to your requirements.
- **Trusted Host**: The device only allows the trusted host to manage the system to enhance the security. Administrator can specify an IP range, MAC address or MAC range, and the hosts in the specified range are the trusted hosts. Only trusted hosts could access the management interface to manage the device.
- **Management Interface**: The device supports the following access methods: Console, Telnet, SSH and WebUI. You can configure the timeout value, port number, PKI trust domain of HTTPS, and PKI trust domain of certificate authentication. When accessing the device through Telnet, SSH, HTTP or HTTPS, if login fails three times in one minute, the IP

address that attempts the login will be blocked for 2 minutes during which the IP address cannot connect to the device.

- **System Time**: You can configure the current system time manually, or synchronize the system time with the NTP server time via NTP protocol.
- **Option**: Specifies system options, including system language, administrator authentication server, host name, password strategy, reboot and exporting the system debugging information.
- **Security Authentication Management**: After you enable Security Authentication Management, SMS or Email two-factor authentication is required for logging in to the device.
- **Storage Management**: The storage management function help you manage system storage space by deleting logs or stopping logging.
- **Password Reset Management**: The password reset function enables you to change passwords through the security question. You can easily reset the password without knowing the previous password. If this function is configured and enabled, when you enter the wrong username or password for three consecutive times through the console port, the system will prompt you to reset the password by the security question.

Administrators

Device administrators of different roles have different privileges. The system supports predefined administrator roles and customized administrator roles. By default, the system supports the following administrators, which cannot be deleted or edited:

- **admin**: Permission for reading, executing and writing. This role has the authority over all features. You can view the current or historical configuration information.
- **admin-read-only**: Permission for reading and executing. You can view the current or historical configuration information.

- **operator**: Permission for reading, executing and writing. You have the authority over all features except modify the Administrator's configuration, view the current or historical configuration information , but no permission to check the log information.
- **auditor**: You can only operate on the log information, including view, export and clear.

The following table shows the permissions to different types of administrators.

Operation	Administratior	Administratior (read-only)	Auditor	Operator
Configure (including saving configuration)	√	χ	χ	√
Configure administrator	√	χ	χ	χ
Restore factory default	√	χ	χ	χ
Delete configuration file	√	χ	χ	√
Roll back configuration	√	χ	χ	√
Reboot	√	χ	χ	χ
View configuration information	√	√	χ	√
View log information	√	√	√	χ
Modify current admin password	√	√	χ	√
ping/traceroute	√	√	χ	√

Notes:

- The device ships with a default administrator named hillstone. You can modify the setting of hillstone.
- Other administrator roles (except default administrator) cannot configure the admin settings, except modifying its own password.
- The system auditor can manage one or more logs, but only the system administrator can manage the log types.

VSYS Administrator

Administrators in different VSYSs are independent from each other. Administrators in the root VSYS are known as root administrators and administrators in the non-root VSYS are known as non-root administrators. The system supports four types of administrator, including Administrators, Administrator(read-only), Operator, and Auditor.

When creating VSYS administrators, you must follow the rules listed below:

- Backslash (\) cannot be used in administrator names.
- The non-root administrators are created by root administrators or root operators after logging into the non-root VSYS.
- After logging into the root VSYS, the root administrators can switch to the non-root VSYS and configure it.
- Non-root administrators can enter the corresponding non-root VSYS after a successful login, but the non-root administrators cannot switch to the root VSYS.
- Each administrator name should be unique in the VSYS it belongs to, while administrator names can be the same in different VSYSs. In such a case, when logging in, you must specify

the VSYS the administrator belongs to in form of vsys_name\admin_name. If no VSYS is specified, you will enter the root VSYS.

The following table shows the permissions to different types of VSYS administrators.

Operation	Root VSYS Administratior	Root VSYS Administratior (read-only)	Root VSYS Auditor	Root VSYS Operator	Non-root VSYS Administratior	Non-root VSYS Administratior (read-only)	Non-root VSYS Operator	Non-root VSYS Auditor
Configure (including saving configuration)	√	χ	χ	√	√	χ	√	χ
Configure administrator	√	χ	χ	χ	√	χ	χ	χ
Restore factory default	√	χ	χ	χ	χ	χ	χ	χ
Delete configuration file	√	χ	χ	√	√	χ	√	χ
Roll back con-	√	χ	χ	√	√	χ	√	χ

Operation	Root VSYS Admin-istratior	Root VSYS Admin-istratior (read-only)	Root VSY-S Aud-itor	Root VSYS Oper-ator	Non-root VSYS Admin-istratior	Non-root VSYS Admin-istratior (read-only)	Non-root VSYS Oper-ator	Non-root VSY-S Aud-itor
figuration								
Reboot	√	χ	χ	χ	χ	χ	χ	χ
View con-figuration inform-ation	√	√	χ	√	View inform-ation in current VSYS	View inform-ation in current VSYS	View inform-ation in current VSYS	χ
View log inform-ation	√	√	√	χ	√	√	χ	√
Modify current admin password	√	√	√	√	√	√	√	√
ping/trace-route	√	√	χ	√	χ	χ	χ	χ

Configuring an Administrator

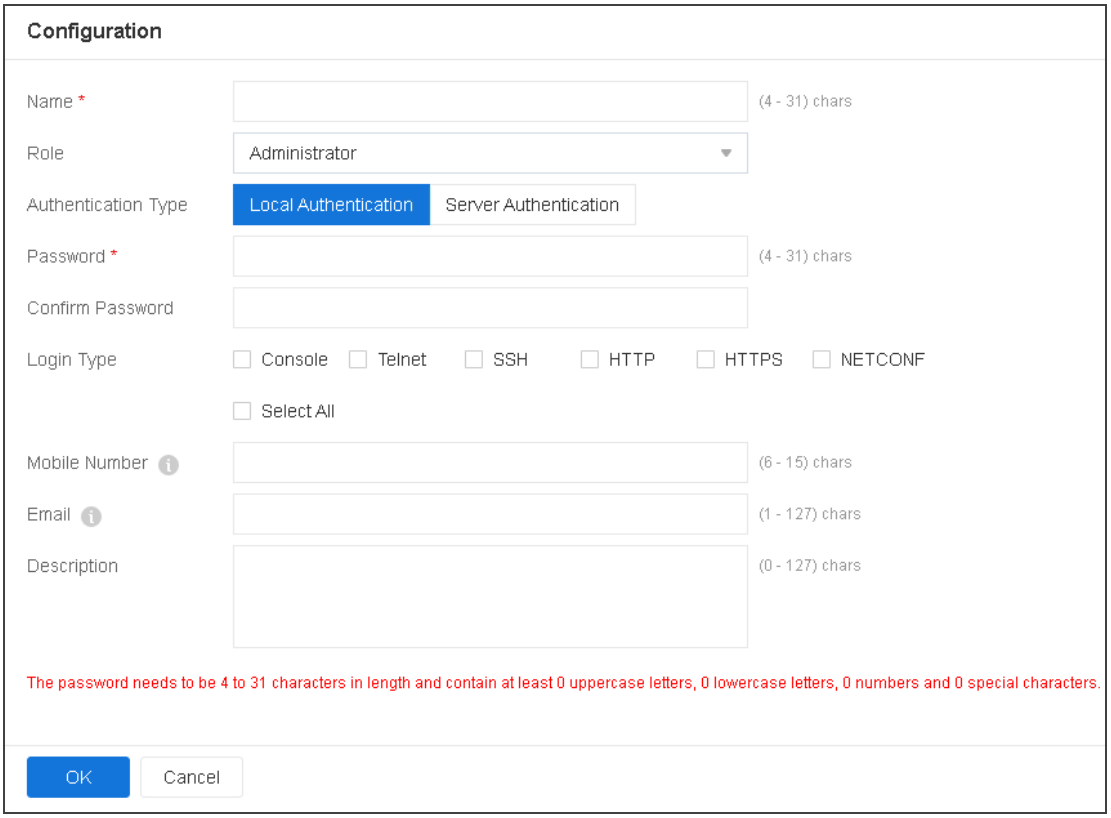
Creating an Administrator Account

To create an administrator account, take the following steps:

1. Select **System** > **Device Management** > **Administrators**.

2. Click **New**.

3. In the **Configuration** dialog box, configure the following.



Option	Description
Name	Type a name for the system administrator account.
Role	From the **Role** drop-down list, select a role for the administrator account. Different roles have different privileges. • Administrator: Permission for reading, executing and writing. This role has the authority over all features. • Operator: This role has the authority over all features except modifying the Administrator's configurations,

Option	Description
	and has no permission to check the log information • Auditor: You can only operate on the log information, including the view, export and clear. • Administrator-read-only: Permission for reading and executing. You can view the current or historical configuration information.
Authentication Type	Select the authentication type, including: • Local Authentication: When an administrator accesses StoneOS, the administrator is authenticated based on the administrator information (including the account and password) configured in StoneOS. • Server Authentication: When an administrator accesses StoneOS, the administrator is authenticated based on the administrator information (including the account and password) configured on the authentication server.
Authentication Server	If **Authentication Type** is set to **Server Authentication**, you need to select an authentication server from the drop-down list or click ⊕ to create an authentication server. For details, see AAA Server. The following servers are supported: • Radius Server • Active Directory Server • LDAP Server

Option	Description
	• TACACS+ Server
Retry Local	After this function is enabled, local password verification will be performed if the server is unreachable. If the server returns the notification of the password error to StoneOS, this function is invalid. By default, the function is disabled.
Password	Type a login password for the admin into the **Password** box. The password should meet the requirements of Password Strategy.
Confirm Password	Re-type the password into the **Confirm Password** box.
Login Type	Select the access method(s) for the admin, including Console, Telnet, SSH, HTTP, HTTPS, and NETCONF. If you need all access methods, select **Select All**.
Mobile Number	Enter a mobile number. After the SMS authentication is enabled, the administrator who does not configure the mobile number will be unable to log in to the device. For more information, see Security Authentication Management.
Email	Enter an email address. After the Email authentication is enabled, the administrator who does not configure the email address will be unable to log in to the device. For more information, see Security Authentication Management.
Description	Enter descriptions for the administrator account.

4. Click **OK**.

Notes: If you select the **Local Authentication Model** on the **Option** page, you need to configure the administrator and authentication information.

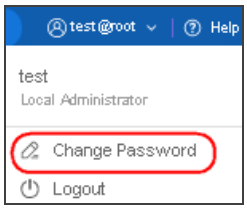
Changing the Password for Admin Users

Device administrators can change the password of other admin users (including other administrators, operators and auditors) by editing the users. To change the password of other admin users, take the following steps:

1. Select **System** > **Device Management** > **Administrators**.
2. Select the admin users from the user list, click **Edit** and change the password in the Configuration page.

Admin users can change their own password by clicking the user name in the top-right corner. To change the password, , take the following steps:

1. Click the user icon or user name in the top-right corner, and select **Change Password** from the drop-down list.



2. In the Password Configuration page, enter the old password and the new one. The new password should be set in accordance with the password policy.



Notes: If the old password is entered incorrectly three times in one minute, the user will be locked for two minutes during which the user cannot change the passwords.

3. Click **OK**.

Configuring Login Options for the Default Administrator

System has a default administrator "hillstone" and a default password "hillstone". However, there is a risk that the default username and password may be cracked. To avoid that risk, when you logs in with the default username and password for the first time, the system will prompt to change the default password. Then, you can log in again with the new password.

Notes: In the HA Active-Passive (A/P) mode, the backup device does not support this function, and you can log in with the default username and password.

Enabling Telnet/HTTP Login Type for the Default Administrator

Admin users can access the device via Console, Telnet, SSH, HTTP or HTTPS. By default, The Telnet and HTTP login types for the default administrator "hillstone" are disabled. To enable the Telnet or HTTP login type for the default administrator, take the following steps:

1. Select **System** > **Device Management** > **Administrators**.

2. Select "hillstone" from the user list, and click **Edit** to open the Configuration page.

3. Select **Telnet** or **HTTP** .

4. Click **OK**.



Notes: When the "Telnet" or "HTTP" login type is enabled, the system will prompt the protocols are not secure.

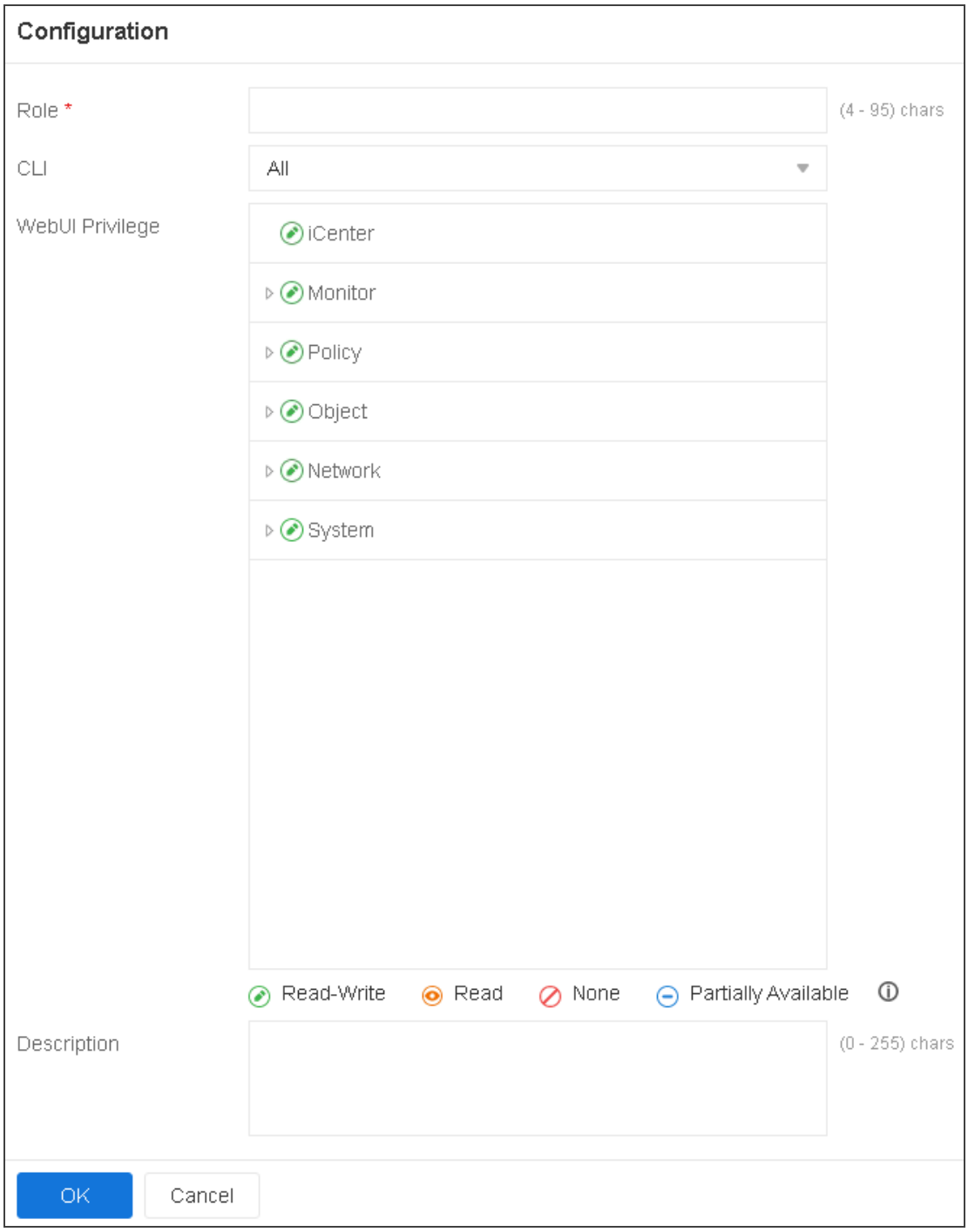
Admin Roles

Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles. The pre-defined administrator role cannot be deleted or edited. You can customize administrator roles according to your requirements:

To create a new administrator role, take the following steps:

1. Select **System > Device Management > Admin Roles**.

2. Click **New**.



3. In the Configuration dialog box, configure the following:

Option	Description
Role	Enter the role name.
CLI	Specify the administrator role's privileges of CLI.
WebUI Privilege	Click module name to set the administrator role's privilege. represents the administrator role does not have privilege of the specified module, and cannot read and edit the configurations of the specified module. represents the administrator role has the read privilege of the specified module, and cannot edit the configurations. represents the administrator role can read and edit the configurations of the specified module.
Description	Specify the description for this administrator role.

4. Click **OK** to save the settings.

Trusted Host

The device only allows the trusted host to manage the system to enhance the security. Administrator can specify an IP range, MAC address or MAC range, and the hosts in the specified range are the trusted hosts. Only trusted hosts could access the management interface to manage the device.



Notes:

- If system cannot be managed remotely, check the trusted host configurations.
- System allows users to configure 128 trusted hosts at most.

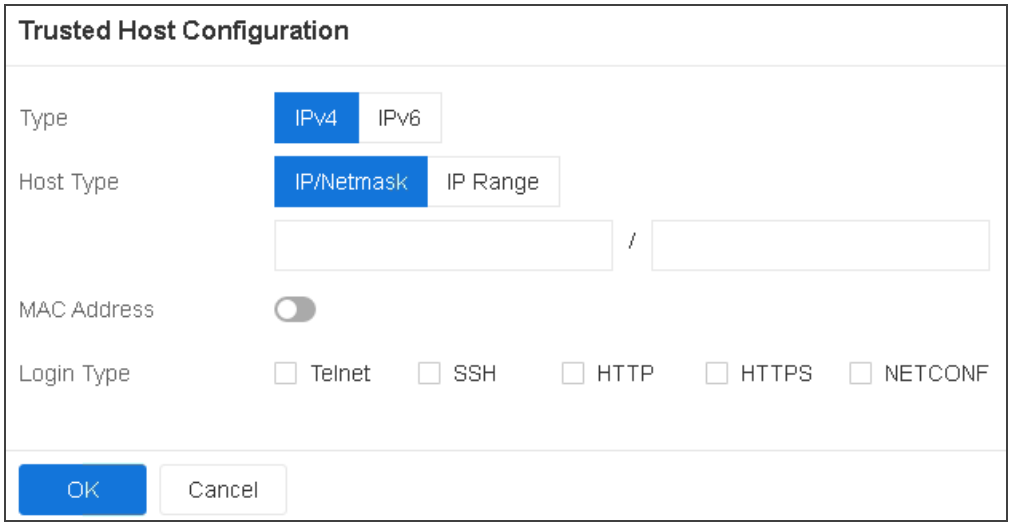
Creating a Trusted Host

To create a trust host, take the following steps:

1. Select **System** > **Device Management** > **Trusted Host**.

2. Click **New**.

3. In the Trusted Host Configuration dialog box, configure these values.



Option	Description
When the system is IPv4 version, configure the following options:	
Match Address Type	Select the address type to match the trusted host. • When "IPv4" is selected, you need to specify the IP range, and only the hosts in the IP range can be the trust hosts; • When "IPv4&MAC" is selected, you need to specify the IP range or MAC address/range, and only the hosts in the specified IP range and MAC range can be the trusted hosts.
IP Type	Specify the IP range of the trusted hosts: • IP/Netmask: Type the IP address and netmask of the trus-

Option	Description
	ted hosts. • IP Range: Type the start IP and end IP of the trusted hosts.
MAC Type	Specifies the MAC address or MAC range of the trusted hosts: • MAC Address: Type the MAC address of the trusted hosts. • MAC Range: Type the start MAC address and end MAC address of the trusted hosts.
Login Type	Select the access methods for the trusted host, including "Telnet", "SSH", "HTTP", "HTTPS", and "NETCONF".
When the system is IPv6 version, configure the following options:	
Type	Select the address type to match the trusted host: "IPv4" or "IPv6".

Host Type	Configure the IPv6 trusted host or the IPv4 trusted host.
	• If the user chooses "IPv4" type, specify the IP address or the IP range of the IPv4 trusted host:
	  • IP/Netmask: Type the IP address and netmask of the trusted hosts.
	  • IP Range: Type the start IP and end IP of the trusted hosts.
	• If the user chooses "IPv6" type, specify the IPv6 address

Option	Description
	or the IPv6 range of the IPv6 trusted host: • IPv6/Prefix: Type the IPv6 address and prefix of the trusted hosts. • IPv6 Range: Type the start IPv6 address and end IPv6 address of the trusted hosts.
MAC Address	Click the **Enable** button to use the MAC address or the MAC range to match the trusted host. By default, this button is disabled.
MAC Type	Specifies the MAC address or the MAC range of the trusted host. • MAC address: Type the MAC address of the trusted hosts. • MAC range: Type the start MAC address and end MAC address of the trusted hosts.
Login Type	Select the access methods for the trust host, including "Telnet", "SSH", "HTTP", "HTTPS" and "NETCONF".

4. Click **OK**.

Management Interface

The device supports the following access methods: Console, Telnet, SSH and WebUI. You can configure the timeout value, port number, PKI trust domain of HTTPS, and PKI trust domain of certificate authentication. When accessing the device through Telnet, SSH, HTTP or HTTPS, if login fails three times in one minute, the IP address that attempts the login will be blocked for 2 minutes during which the IP address cannot connect to the device.

To configure the access methods:

1. Select **System** > **Device Management** > **Management Interface**.

2. In the Management Interface tab, configure these values.

Option	Description
Console	Configure the Console access method parameters. • Timeout: Type the Console timeout value into the **Timeout** box. The value range is 0 to 60. The default value is 10. The value of 0 indicates never timeout. If there is no activity until the timeout, system will drop the console connection.
Telnet	Configure the Telnet access method parameters. • Timeout: Specifies the Telnet timeout value. The value range is 1 to 60. The default value is 10. • Port: Specifies the Telnet port number. The value range is 1 to 65535. The default value is 23.
SSH	Configure the SSH access method parameters. • Timeout: Specifies the SSH timeout value. The value range is 1 to 60. The default value is 10. • Port: Specifies the SSH port number. The value range is 1 to 65535. The default value is 22.
Web	Configure the WebUI access method parameters. • Multiple Login with Same Account: Select the check box and users are allowed to log in to devices with the same account simultaneously. By default, the function is dis-

Option	Description
	abled. In the default situation, when a same account is used to log in again, the previous login account will be kicked out. • Timeout: Specifies the WebUI timeout value. The value range is 1 to 1440. The default value is 10. • HTTP Port: Specifies the HTTP port number. The value range is 1 to 65535. The default value is 80. • HTTPS Port: Specifies the HTTPS port number. The value range is 1 to 65535. The default value is 443. • HTTPS Trust Domain: Select the configured PKI trust domain from the dropdown list. When users access the device via HTTPS, in the SSL authentication process, the HTTPS server uses the certificate stored in the specified PKI trust domain. • Certificate Authentication: With this checkbox selected, The system enables the certificate authentication of the client. The certificate includes the digital certificate of users and secondary CA certificate signed by the root CA.Certificate authentication is one of two-factor authentication. The two-factor authentication does not only need the user's name and password authentication, but also needs other authentication methods, like a certificate or fingerprint.

Option	Description
	• Certificate Trust Domain: After enabling the certificate authentication and logging into the device over HTTPS, the system verifies the validity of the CA signature of the certificate in the client by using the CA root certificate stored in this PKI trust domain. Make sure that root CA certificate is imported into it. • CN Check: After the CN Check function is enabled, the system checks the CN field of the client certificate when the user logs into the device. Only when the CN field of the client certificate matches the username can the user successfully log into the device.

3. Click **OK**.



Notes: When changing HTTP port, HTTPS port or HTTPS Trust Domain, the web server will restart. You may need to log in again if you are using the Web interface.

System Time

You can configure the current system time manually, or synchronize the system time with the NTP server time via NTP protocol.

Configuring the System Time Manually

To configure the system time manually, take the following steps:

1. Select **System** > **Device Management** > **System Time**.

2. Under System Time Configuration in the System Time tab, configure the following.

Option	Description
Sync with Local PC	Specifies the method of synchronize with local PC. You can select **Sync Time** or **Sync Zone&Time**. • Sync Time: Synchronize the system time with local PC. • Sync Zone&Time: Synchronize the system zone&time with local PC.
Specified the system time.	Configure parameter of system time. • Time Zone: Select the time zone from the drop-down list. • Date: Specifies the date. • Time: Specifies the time.

3. Click **OK**.

Configuring NTP

The system time may affect the establishment time of VPN tunnel and the schedule, so the accuracy of the system time is very important. To ensure the system is able to maintain an accurate time, the device allows you to synchronize the system time with a NTP server on the network via NTP protocol.

To configure NTP:

1. Select **System** > **Device Management** > **System Time**.

2. Under NTP Configuration in the System Time tab, configure the following.

Option	Description
Enable	Select the **Enable** check box to enable the NTP function. By default, the NTP function is disabled.
Authentication	Select the **Authentication** check box to enable the NTP Authentication function.
Server	Specifies the NTP server that device need to synchronize with. You can specify at most 3 servers. • IP: Type IP address of the server . • Key: Select a key from the **Key** drop-down list. If you enable the NTP Authentication function, you must specify a key. • Virtual Router: Select the Virtual Router of interface for NTP communication from the drop-down list. • Source interface: Select an interface for sending and receiving NTP packets. • Specify as a preferred server: Click **Specify as a preferred server** to set the server as the first preferred server. The system will synchronizate with the first preferred server.
Sync Interval	Type the interval value. The device will synchronize the system time with the NTP server at the interval you specified to

Option	Description
	ensure the system time is accurate.
Time Offset	Type the time value. If the time difference between the system time and the NTP server's time is within the max adjustment value you specified, the synchronization will succeed, otherwise it will fail.

3. Click **OK**.

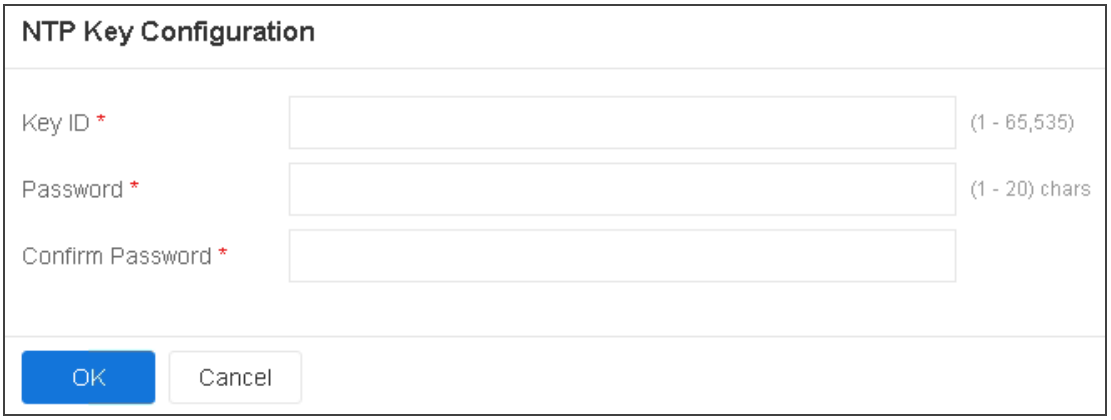
NTP Key

After enabling NTP Authentication function, you need to configure MD5 key ID and keys. The device will only synchronize with the authorized servers.

Creating a NTP Key

To create an NTP key:

1. Select **System** > **Device Management** > **NTP Key**.
2. Click **NEW**.
3. In the NTP Key Configuration dialog box, configure these values.



Option	Description
Key ID	Type the ID number into the Key ID box. The value range is 1 to 65535.
Password	Type a MD5 key into the **Password** box. The value range is 1 to 31.
Confirm Password	Re-type the same MD5 key you have entered into the **Confirm** box.

4. Click **OK**.

Option

Specifies system options, including system language, administrator authentication server, host name, password strategy, reboot, exporting the system debugging information, enabling application layer security bypass, and enabling the configuration audit function.

To change system option, take the following steps:

1. Select **System** > **Device Management** > **Settings & Options**.
2. Select **System Settings** .Configure the following.

Option	Description
Hostname	Type a host name you want to change into the **Hostname** box.

Option	Description
Domain	Type a domain name you want to specify into the **Domain** box.
Title Display Mode	Configure the browser tab title at WebUI login. You can configure the host name, platform and management address as the tab title. Multiple items can be selected. The sequence of these items displayed in the actual tab title is consistent with the selection sequence. The default title is "Hillstone Networks".
System Language	You can select **Chinese** or **English** according to your own requirements.
Authentication Model	Select the authentication model, including: • Local Authentication Model: After **Local Authentication Model** is configured, you need to configure administrator and authentication information. • Server Authentication Model: After **Server Authentication Model** is configured, you need to configure administrator and authentication information.
Authentication Server	If **Authentication Model** is set to **Server Authentication Model**, you need to select an authentication server from the drop-down list or click ⊕ to create an authentication server. For details, see AAA Server. The following servers are supported: • Radius Server • TACACS+ Server

Option	Description
Local Password Retry	After this function is enabled, local password verification will be performed if the server returns the notification of the password error to StoneOS. If the server is unreachable, the StoneOS system will enable the **Local Password Retry** by default. By default, the function is enabled.
Lock IP	
Maximum count of login attempts	Specify the maximum number of login attempts of an IP. The value range is from 0 to 256. The default value is 256.
Locking Time	Specify the locking time of the lock IP. The value range is 1 to 65535 minutes, and the default value is 2 minutes.
Lock Account	
Maximum count of login attempts	Specify the maximum number of login attempts of an account. The value range is from 1 to 5. The default value is 3.
Locking Time	Specify the locking time of the lock account. The value range is 1 to 65535 minutes, and the default value is 2 minutes.
Minimum Password Length	Specifies the minimum length of password. The value range is 4 to 16 characters. The default value is 4.
Password Complexity	**None** means no restriction on the selection of password characters. You can select **Password Complexity Settings** to enable password complexity checking and configure password complexity.

Option	Description
	• Minimum Capital letters length: The default value is 2 and the range is 0 to 16. • Minimum Lowercase Letter Length: The default value is 2 and the range is 0 to 16. • Minimum Number Length: The default value is 2 and the range is 0 to 16. • Minimum Special Character Length: The default value is 2 and the range is 0 to 16. • Validity Period: The unit is day.The range is 0 to 365.The default value is 0, which indicates that there is no restriction on validity period of the password.
History Password Check	The system supports the History Password Check function to ensure the security of passwords. With this function enabled, when you change your password, the system verifies that whether the new password is the same as the historical password. If your new password is the same as the historical password, the prompt "The new password cannot be the same as the old one" appears, reminding you of re-entering another new password. Click the enable button to enable History Password Check function and specify the number of historical passwords to be verified. The value rage is from 3 to 8. The default value is 5, indicating that the new password cannot be the same as the

Option	Description
	last five historical passwords.

3. Click **OK**.

Rebooting the System

Some operations like license installation or image upgrading will require the system to reboot before it can take effect.

To reboot a system, take the following steps:

1. Go to **System > Device Management> Settings & Options** .
2. In the **System Options** page, click **Reboot**, and select **Yes** in the prompt.
3. The system will reboot. You need to wait a while before it can start again.

System Debug

The system provides failure feedback and system debugging information functions, which help you to identify and analyze issues. For more information, see "Debugging" on Page 1652.

Application Layer Security Bypass

System supports to bypass the application layer functions, including Intrusion Prevention System, Anti Virus, and other application layer security protection function.

To enable application layer security bypass, take the following steps:

1. Select **System > Device Management> Settings & Options**.
2. In the **System Settings** page, select the **Enable** button for application layer security bypass, and click **OK**.

Storage Management

The system provides storage management functions to help you manage system storage space by limiting the disk space occupied by each function. In addition, system allocates fixed storage space for packet loss statistics, long-term monitor, reports, and logs of each module. For devices with hard disks installed, you can configure a custom storage size. When the data storage space of each function reaches or exceeds the configured thresholds, logs are generated to generate alarms. The configuration of the storage management page varies depending on whether the device contains hard disks.



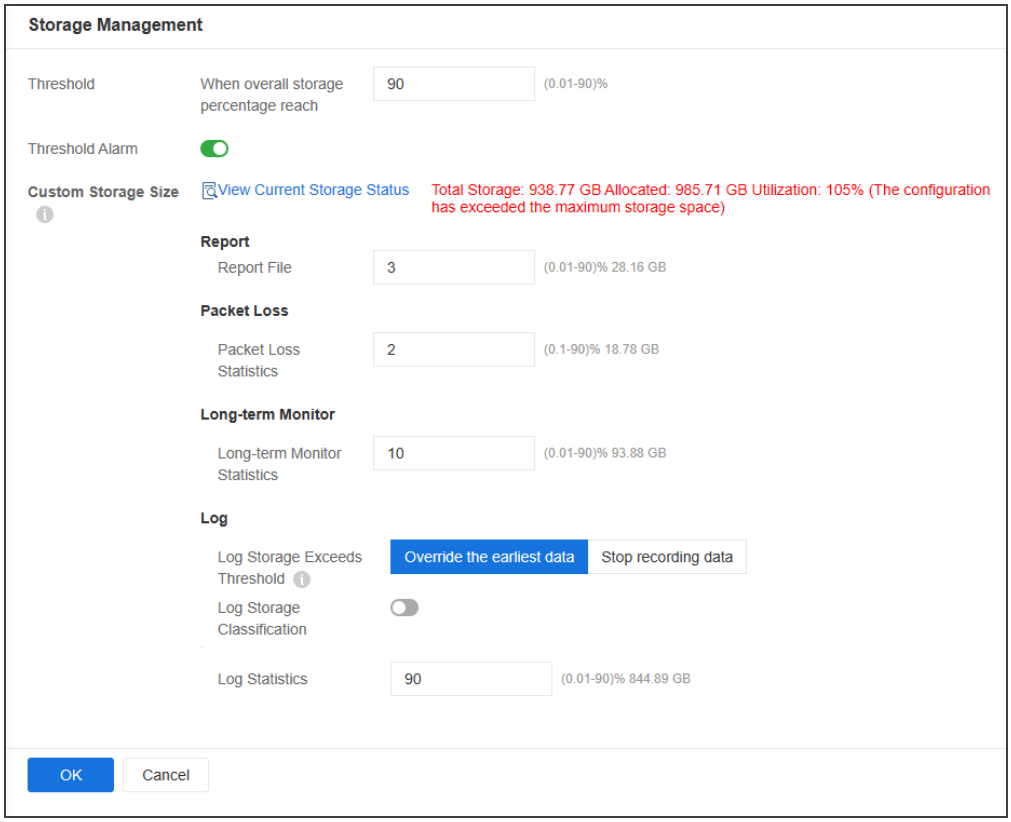
Notes:

- The storage management function is available only for:
  - SG-6000 A-Series devices (except SG-6000-A200/A200W/A200G4B)
- It is recommended that the sum of custom storage space configurations do not exceed the total threshold. Otherwise, some data stores may fail to reach the preset threshold.

To configure the storage management function, take the following step:

1. Select **System > Device Management > Storage Management**.

2. For devices installed with hard disks., configure the following options:

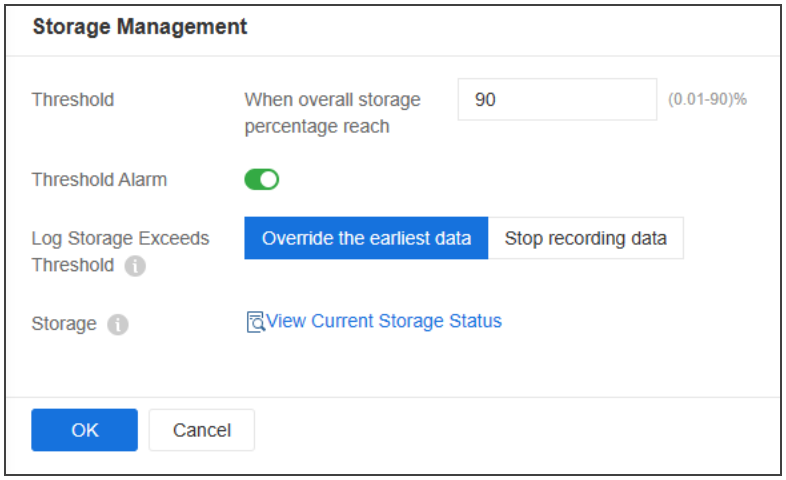


Option	Description
Threshold	When the system storage ratio reaches the specified threshold, the system will perform the specified action to control the system storage. The storage ratio ranges from 1% to 90%.
Threshold Alarm	When the system storage ratio or storage space reaches the specified threshold, the system will record a log message.
Custom Storage Size	
View Current Storage Status	Show the Total Storage, Allocated Storage and Utilization. Click **View Current Storage Status** to view maximum storage space

Option	Description
	and utilization of each module log and report files.
Packet Loss	
Packet Loss Statistics	Specifies the storage size for statistical data of packet loss of functional modules. A default storage size is allocated to the statistical data. You can customize the storage size. If the storage usage exceeds the specified threshold, earlier statistical data is deleted. **Note**: The Packet Loss function is available only for: SG-6000 A-Series devices (except A1605/A1805/A2205) installed with hard disks.
Report	
Report File	Specifies the disk space size of the report file. The system allocates a default disk space size for the report file, and you can customize the disk space size for the report file as needed. If the storage usage exceeds the specified threshold, earlier statistical data is deleted.
Long-term Monitor	
Long-term Monitor Statistics	Specifies the storage size for statistical data of the Long-term Monitor function. The system allocates default storage size to long-term monitor statistics. You can customize the storage size. If the storage usage exceeds the specified threshold, earlier statistical data is deleted. The long-term monitor function is available only for: • SG-6000 A-Series devices (except

Option	Description
	A1605/A1805/A2205) installed with hard disks. • .
Log	
Log Storage Exceeds Threshold	This option takes effect only for log storage. When reached the specified threshold, the system will perform the specified action, including override the earliest data and stop recording data. • Override the earliest data: The system will delete earliest logs. • Stop recording data: The system will stop storing new logs.
Log Storage Classification	Click **Enable** button to specify the disk space size of each module log. The system allocates a default disk space size for the log of each module, and you can customize the disk space size for the log as needed.
Log Statistic	Specifies the total storage capacity for all types of logs. **Note**: **Log Statistics** and **Log Storage Classification** are mutually exclusive and cannot be configured at the same time.

3. For devices without hard disk, configure the following options:



Option	Description
Threshold	When the system storage ratio reaches the specified threshold, the system will perform the specified action to control the system storage. The storage ratio ranges from 1% to 90%.
Threshold Alarm	When the system storage ratio or storage space reaches the specified threshold, the system will record a log message.
Log Storage Exceeds Threshold	This option takes effect only for log storage. When reached the specified threshold, the system will perform the specified action, including override the earliest data and stop recording data. • Override the earliest data: The system will delete earliest logs. • Stop recording data: The system will stop storing new logs.
Storage	Show the Total Storage, Allocated Storage and Utilization. Click

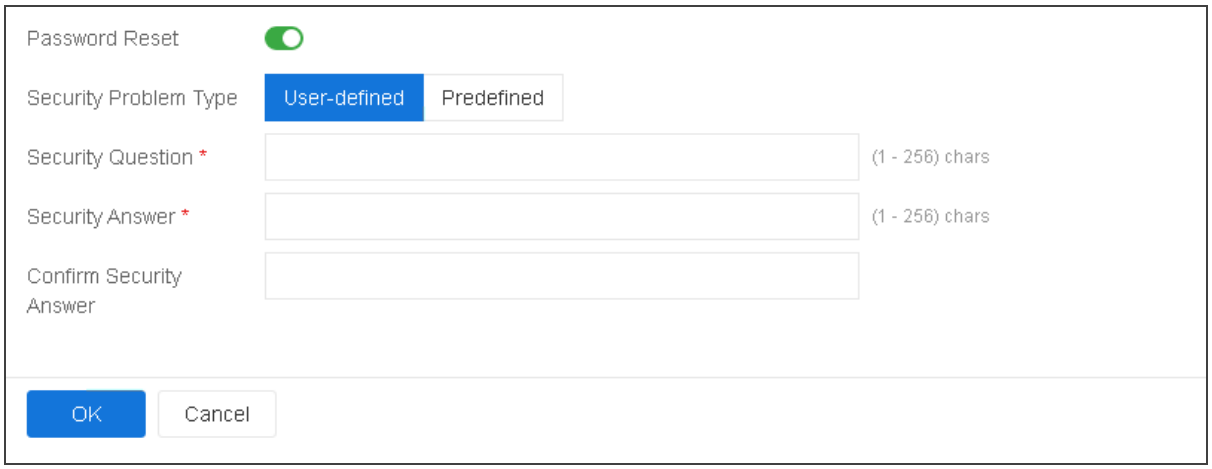
Option	Description
	View Current Storage Status to view maximum storage space and utilization of each module log(Event Log, Configuration Log and Network Log) and report files. **Note**: The maximum storage space for all types of logs and report files is the default disk space allocated by system: Event Log 7%, Configuration Log 6%, Network Log 6%, and report files 20%.

4. Click **OK** to save the settings.

Password Reset Management

The password reset function enables you to change passwords through the security question. You can easily reset the password without knowing the previous password. If this function is configured and enabled, when you enter the wrong username or password for three consecutive times through the console port, the system will prompt you to reset the password by the security question. To configure the password reset function, take the following steps:

1. Select **System** > **Device Management** > **Password Reset Management**.



2. Click the Enable button and configure the following options.

Option	Description
Password Reset	Click the **Enable** button to enable the password reset function.
Security Problem Type	Specify the type of Security Problem as User-defined or Predefined.
Security Question	Configure the security question. If the type of Security Problem is specified as user-defined, enter a user-defined security question in the text box. If the type of Security Problem is specified as predefined, select a predefined security question from the drop-down list. The value range is 1 to 256 characters. The security question can only include letters, numbers, and special characters (excluding "). Chinese characters cannot be included in the security question.
Security Answer	Configure the security answer. The value range is 1 to 256 characters. The security answer can only include letters, numbers, and special characters (excluding "). Chinese characters cannot be included in the security question.
Confirm Security Answer	Enter the security answer again in the text box which must be consistent with the content in the security answer text box.

3. Click **OK**.

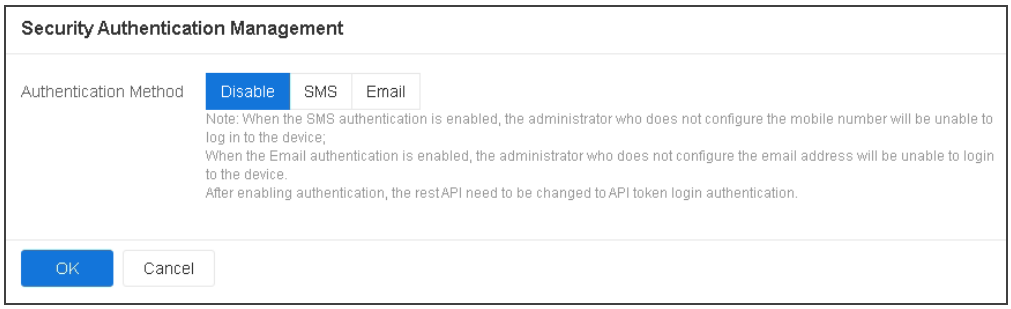
Security Authentication Management

After you enable Security Authentication Management, SMS or Email two-factor authentication is required for logging in to the device.

To enable Security Authentication Management, take the following steps:

1. Select **System** > **Device Management** > **Security Authentication Management**.

2. On the Security Authentication Management page, configure the following options:



Option	Description
Disable	Select **Disable** to disable authentication. By default, this option is selected.
SMS	Select **SMS** to enable the SMS authentication. After the SMS authentication is enabled, the administrator who does not configure the mobile number will be unable to log in to the device. • SMS Authentication: Specifies the method of the SMS authentication. Valid values: SMS Modem and SMS Gateway. If you select **SMS Gateway**, select an SMS gateway from the **SMS Gateway** drop-down list. For more information, see "SMS Parameters" on Page 1828. • Verification Code Timeout: Specifies the validity period of SMS verification codes. Valid values: 1 to 30 minutes. Default value: 5 minutes. You cannot log in to the device if you do not enter the verification code within the validity period. • Sender Name: Specifies the sender name, which can be 1

Option	Description
	to 64 characters. The name will be displayed in the text message.
Email	Select **Email** to enable the Email authentication. After the Email authentication is enabled, the administrator who does not configure the email address will be unable to log in to the device. • Mail Server: Select a mail server from the drop-down list. For more information, see "Mail Server" on Page 1812. • Verification Code Timeout: Specifies the validity period of email verification codes. Valid values: 1 to 30 minutes. Default value: 5 minutes. You cannot log in to the device if you do not enter the verification code within the validity period. • Sender Name: Specifies the sender name, which can be 1 to 64 characters. The name will be displayed in the email.

3. Click **OK**.

Startup Wizard

With the Startup Wizard, you can quickly complete the initialization configuration of the device without the need to delve into complex configuration details. This allows you to connect the device to the internet and achieve basic security protection.

After logging in to the firewall and changing the password via WebUI, you will be presented with a Startup Wizard. You can follow the steps to complete initial configuration of the firewall, including the host name, system time and license, routing mode deployment, and security policy configuration. You can also skip the Startup Wizard and configure the firewall.

Notes:

Under any of the following conditions, the Startup Wizard will not be prompted when the administrator logs in the WebUI:

- The firewall is deployed in HA mode;
- The login address does not point to the WebUI homepage, such as "http://x.x.x.x/#icenter";
- Logging in to the firewall WebUI on the HSM device;
- Logging in to the firewall WebUI via SSO on the cloud platform.

Skipping the Startup Wizard

To skip the Startup Wizard, take the following steps:

1. On the Startup Wizard welcome page, Click **Skip**.
2. The Skip page will be displayed, asking "Are you sure to skip the startup wizard?". You can select the **Do not display next-time login** check box as required. If this check box is not selected, the Startup Wizard will be displayed at your next login.
3. Click **OK** to close the Startup Wizard.

Starting the Startup Wizard

If the Startup Wizard is skipped, you can restart it again as follows:

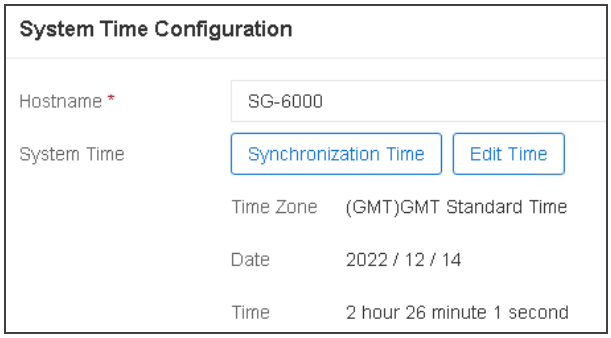
1. Select **System** > **Device Management** > **Startup Wizard**.
2. On the Startup Wizard page, configure whether to restore the device to factory defaults as required:

a. If **Restore to Factory Defaults** is enabled, the system will erase all system configuration after you start the Startup Wizard.

b. If **Restore to Factory Defaults** is disabled, the security policies created in the Startup Wizard have a higher priority than the policies (if any) previously configured in the Policy module. Other configuration, except policies, will be updated to the one configured in the Startup Wizard. By default, **Restore to Factory Defaults** is disabled.

3. Click **Open** to go to the Startup Wizard.

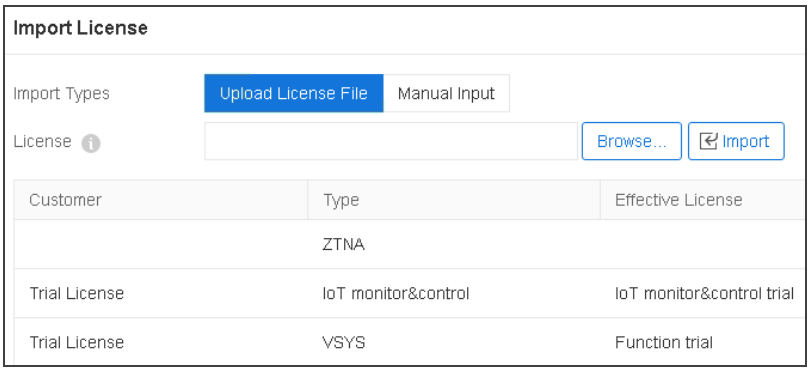
4. Click **Start Wizard** to start the Startup Wizard and enter the **System Time Configuration** page.



Option	Description
Hostname	Type the hostname. The value length is from 1 to 63 characters. The default value is SG-6000. Click **Next** to deploy the configuration.
System Time	Set the system time in either of the following ways: • Click **Synchronization Time** and the corresponding panel appears, where you can view your current timezone. Click **OK**. • Click **Edit Time,** and the corresponding panel appears,

Option	Description
	where you can set the timezone, date and time and then click **OK**.

5. Click **Next** to go to the **Import License** page.



Option	Description
Import Types	Specifies the method to import licenses. When licenses are imported, they are listed on the current page. Note that some licenses take effect only after a system restart. Please restart the system when Startup Wizard is fully configured. There are two ways of importing the licenses: • **Upload License File**: Click **Browse**, select the license that needs to be imported and then click **Import**. • **Manual Input**: Type the license content in the **License** text box and then click **Import**.

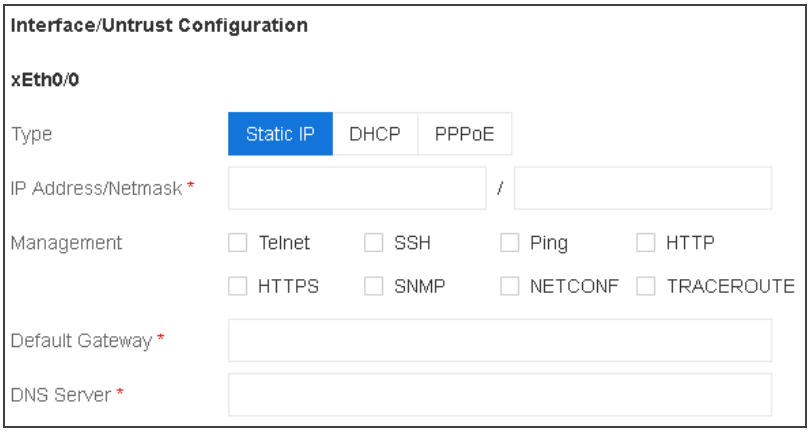
6. Click **Next** to go to the **Network Configuration** page. Network configuration will be deployed when the Startup Wizard is fully configured. In the Network Configuration section, in addition to the configuration that you can manually add in the Startup Wizard, the

system automatically configures an SNAT rule that enables the Sticky function, translating the Intranet IP to the IP address of the Intranet exit IP.



Option	Description
Untrust	Select the Internet interface and add it to the untrust zone.
Trust	Select the Intranet interface and add it to the trust zone.

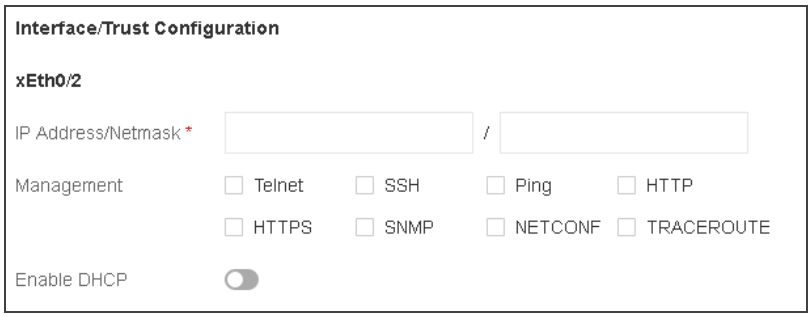
7. Click **Next** and configure the Internet interface.



Option	Description
Type	Select the method of obtaining IP addresses for the Internet interface.
Static IP	Specifies the IP address and netmask for the interface when **Static IP** is selected.
DHCP	When DHCP is selected, the interface will automatically obtain IP addresses using DHCP.
PPPoE	When PPPoE is selected, configure the following parameters:

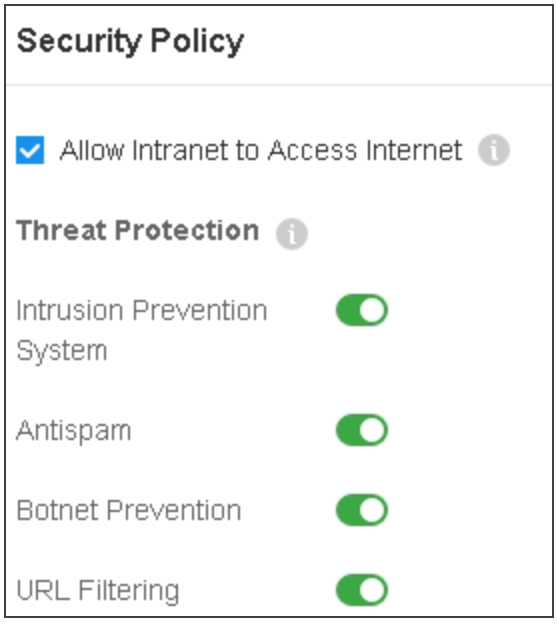
Option	Description
	• User: Specifies the PPPoE user name. The value length is from 1 to 31 characters. • Password: Specifies the password of the PPPoE user. The value length is from 1 to 31 characters. • Confirm Password: Type the password again. • Idle Interval: Specifies the idle interval. The uint is in minutes. The value range from is 0 to 10,000 minutes. When the idle time of the PPPoE interface reaches the specified value, the system will terminate the connection. By default, the value is 0, meaning the connection will not be terminated by the system. • Reconnect Interval: Specifies the interval after which the system will automatically reconnect after a disconnection The unit is in seconds. The value range is from 1 to 10,000 seconds.
Management	Specifies the interface management method, including Telnet, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.
Default Gate-way	Specifies the default gateway address.
DNS Server	Specifies the DNS server address.

8. Click **Next** to configure the Intranet interface.



Option	Description
IP Address/Net-mask	Specifies the IP address and netmask of the interface.
Management	Specifies the interface management method, including Tel-net, SSH, Ping, HTTP, HTTPS, SNMP, NETCONF and TRACEROUTE.
Enable DHCP	After DHCP service is enabled, the interface will be con-figured as a DHCP server.
DHCP lease range	Specifies the address pool range. After the interface is con-figured as a DHCP server, the system will assign IP addresses from the address pool to the hosts, attempting to connect the interface.

9. Click **Next** to go to the **Security Policy** page. Security policy configuration will be deployed when the Startup Wizard is fully configured.



Option	Description
Allow Intranet to Access Internet	Select this check box to configure a security policy from the source zone (trust) to the destination zone (untrust), which will allow Intranet users to access the Internet. If this check box is not selected, the security policy will not be created.
Threat Protection	After **Allow Intranet to Access Internet** is selected, enable threat prevention functions as required. The threat prevention functions take effect only after corresponding licenses are imported. Initially, enabled threat prevention functions apply their default profile. To configure specific profiles, navigate to related modules after the Startup Wizard is fully configured. Note that some

Option	Description
	licenses take effect after a system reboot.

10. Click **Next** to go to the **Connecting to Hillstone Cloud Service Platform** page. Select the **Join the User Experience Program** check box to connect the system to the default Hillstone Cloud Platform account. This way, the system obtains broader threat intelligence so as to improve its protection capability.



11. Click **Next** to go to the **Options** page. You can view all configurations configured via the Startup Wizard.

12. Make sure the configurations are correct. Click **OK** to deploy network configuration and security policy configuration.

Configuration File Management

System configuration information is stored in the configuration file, and it is stored and displayed in the format of command line. The information that is used to initialize the Hillstone device in the configuration file is known as the initial configuration information. If the initial configuration information is not found, the Hillstone device will use the default parameters for the initialization. The information being taking effect is known as the current configuration information.

System initial configuration information includes current initial configuration information (used when the system starts) and backup initial configuration information. System records the latest ten saved configuration information, and the most recently saved configuration information for the system will be recorded as the current initial configuration information. The current configuration information is marked as "Startup"; the previous nine configuration information is marked with number from 0 to 8, in the order of save time.

You can not only export or delete the saved configuration files, but also export the current system configurations.

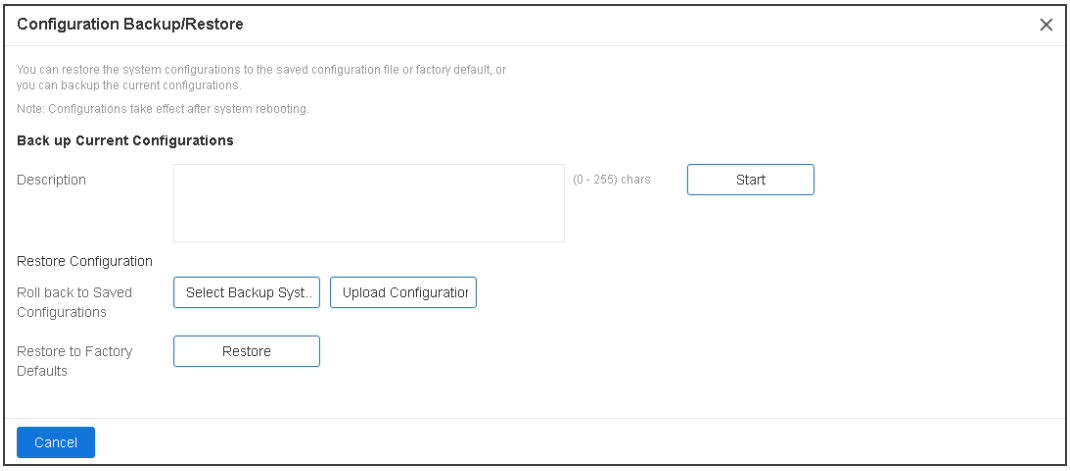
Notes: If you have rolled back to a specified saved initial configuration, the configuration information is marked as "Startup".

Managing Configuration File

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

To manage the system configuration files, take the following steps:

1. Select **System** > **Configuration File Management** > **Configuration File List**.
2. In the Configuration File List page, configure the following.
   - Export: Select the configuration file you want to export, and click **Export**. You can export DAT and ZIP files. For the ZIP type, you can set a compression password as required.
   - Delete: Select the configuration file you want to delete, and click **Delete**.
   - Backup Restore: You can restore the system configurations to the saved configuration file or factory default, or you can backup the current configurations.



Option	Description
Back up Current Configurations	Type descriptions for the configuration file into **Description** box. Click **Start** to backup.
Restore Configuration	Roll back to Saved Configurations: • Select Backup System Configuration File: Click this button, then select Backup Configuration File from the list. Click **OK**. • Upload Configuration File: Click this button. In the Importing Configuration File dialog box, click **Browse** and choose a local configuration file you need in your PC. If you need to make the configuration file take effect, select the check box. Click **OK**. You can upload DAT and ZIP files. For the encrypted ZIP file, you need to enter the compression password. Restore to Factory Defaults: • Click **Restore**, in the Restore to Factory Defaults dialog box, click **OK**.

Notes: Device will be restored to factory defaults. Meanwhile, all the system configurations will be cleared, including backup system configuration files.

Viewing the Current Configuration

To view the current configuration file:

1. Select **System** > **Configuration File Management** > **Current Configurations**.
2. Click **Export** to export the current configuration file.

Importing/Exporting the Configuration of All VSYS

You can export the current configuration file of VSYS, and import the saved configuration file of VSYS.

To export the current configuration file of VSYS, take the following steps:

1. Select **System > Configuration File Management > Configuration File List**.
2. Click **Export All Vsys Configuration** to export the current configuration file of VSYS.

To import the saved configuration file of VSYS, take the following steps:

1. Select **System > Configuration File Management > Configuration File List**.
2. Click **Import All Vsys Configuration** .
3. Click **Brown** to select the configuration file needed to be imported. The file type can be GZ and ZIP.
4. After importing the configuration file, you need to reboot to take effect. Select the **Restart now**, make the new configuration take effect checkbox to reboot immediately.
5. Click **OK**.

Docker Management

Docker is an open-source platform that allows developers to package applications and their dependencies into lightweight, portable containers. By utilizing containerization, Docker enables developers to isolate applications, eliminate environment inconsistencies, and streamline the deployment process.

StoneOS supports the Docker management function. By using this function, you can create a Docker, allocate system resources in the system, import Docker image files, and run container applications based on Docker.

Operations about Docker Management

You can perform the following operations about Docker management:

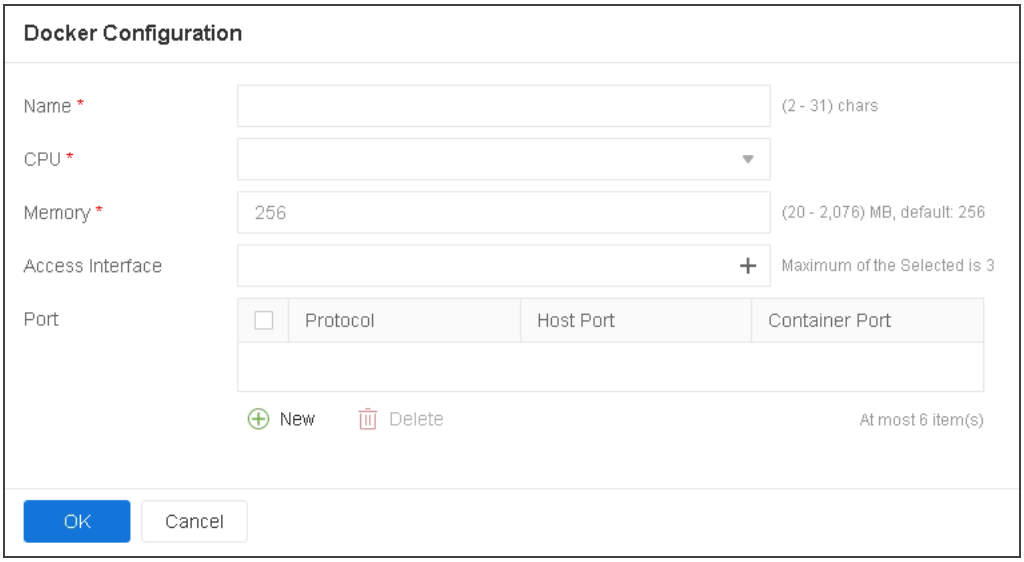
- Creating a Docker and Allocating System Resources
- Editing/Deleting a Docker
- Managing Image Files
- Managing a Container
- Docker Global Configuration

Creating a Docker and Allocating System Resources

In StoneOS, all Docker instances share CPU, memory, and port resources of the system. You can allocate CPU, memory, and port resources for each Docker instance.

To create a Docker and allocate system resources for the Docker, take the following steps:

1. Select **System** > **Docker Management** > **Docker**.
2. Click **New**.



Option	Description
Name	Specifies the name of the Docker, which needs to be a string that contains 2 to 32 letters or numbers.
CPU	Select the CPU core to which the Docker is bound from the drop-down list. **Note**: By default, the newly created Docker is bound to Core0. To prevent that Core0 is in a highly loaded state when the container is running, you can use the **flow-core-num** *number* command to release the CPU cores occupied at the data layer. This way, the Docker can use the CPU cores. For example, if the total number of CPU cores is 8 (Core0~Core7), you can use the **flow-core-num 4** command to specify that the data layer occupies 4 CPU cores (Core0~Core3), and the remaining Core4~Core7 are the CPU cores that can be bound by Docker. For a device that contains only 2 CPU cores, the Docker can only be bound to Core0 because the system does not support the **flow-core-num** *number* command.
Access Inter-face	Specifies the name of the interface used to access the Docker. To do this, click "+" and select an interface name (except MGT interface and HA interface) from the interface list. You can select at most 3 interfaces.
Memory	Specifies the maximum memory that can be used by the Docker. By default, the maximum memory that can be used is 256 MB.
Port	Specifies the port mapping of Docker communication. To do this, select a protocol type of port from the **Protocol** drop-down list, select a host port number of the **Docker** from the **Host Port** drop-down list, and select a Docker port number from the **Con-**

Option	Description
	tainer Port drop-down list. **Note**: When you create a Docker for the IoT asset identification system, the container port number needs to be 45622.

3. Click **OK**. The newly created Docker is displayed in the Docker list.



Notes:

- To ensure the normal operation of other system functions, we recommend that you allocate CPU and memory resources for Docker based on the resource utilization of the Docker.
- The number of Dockers that can be created varies based on platform:
  - For SG-6000-A5100 and above, you can create at most 3 Dockers; For devices that are below SG-6000-A5100, you can create at most 1 Docker. For SG-6000-A2200/A1800/A1600/A200/A200G4/A200W/A200WG4, you cannot create a Docker.

Editing/Deleting a Docker

To edit or delete a Docker, take the following steps:

1. Select **System** > **Docker Management** > **Docker**.
2. Select the Docker that you want to edit or delete from the list.
3. Click **Edit** or **Delete**. When you delete the Docker, container and image files within the Docker are deleted at the same time.

Managing Image Files

You can manage Docker image files, including importing image files, viewing imported image files, deleting image files, replacing image files, or setting an image file as first preference.

Select **System** > **Docker Management** > **Docker**. On the **Docker** page, you can perform the following operations on image files:

- Import image file: Click ⋮ and select **Import image file**. In the **Import** panel, click **Browse**, select an image file, and click **OK**.
- View imported image files: Click ⋮ and select **Operate image files**. In the **Image File** panel, view the name and type of imported image files. You can also click **Import** to import an image file.
- Delete an image file: Click ⋮ and select **Operate image files**. In the **Image File** panel, find the image file that you want to delete and click **Delete** in the **Operation** column. The image file that is in use cannot be deleted.
- Replace an image file: Click ⋮ and select **Operate image files**. In the **Image File** panel, find the image file that you want to replace and click **Import & Replace** in the **Operation** column. In the **Import & Replace** panel, import a new image file to replace the current one. The image file that is in use cannot be replaced.
- Set am image file as first preference: Click ⋮ and select **Operate image files**. In the **Image File** panel, turn on the switch in the **First Preference** column. After you set the image file as first preference, when the device restarts, it preferentially selects this image file for loading.



Notes: You can import at most 3 image files for each Docker.

Managing a Container

You can manage containers in use in Docker, including running, reloading, stopping, starting, restarting, or replacing a container.

Select **System** > **Docker Management** > **Docker**. On the **Docker** page, you can perform the following operations on containers:

- Run a container: If no container is created, click ⋮ and select **Run** to load the specified image file and run the container.
- Reload a container: If a container is created, click ⋮ and select **Reload** to delete the existing container, load the image file, and then run the container.
- Stop a container: Click **Stop** in the **Operation** column to stop the container in use.
- Start a container: Click **Start** in the **Operation** column to start the container that is stopped.
- Restart a container: Click ⋮ and select **Reboot** to restart the container in use.
- Remove a container: Click ⋮ and select **Remove Container** to remove the container.

Docker Global Configuration

The Docker global configuration includes the network segment address configuration of Docker. Docker connects a container network to host network via a bridge. You need to configure the network segment address of Docker. The available IP addresses within this network segment will be used for internal interfaces of the host network and container. If no network segment address of Docker is configured, Docker cannot be used.

To configure the network segment address of Docker, take the following steps:

1. Select **System** > **Docker Management** > **Configuration**.



2. In the **IP/Netmask** field, enter the IPv4 address and subnet mask of the network segment of Docker.

3. In the **IPv6/Prefix** field, enter the IPv6 address and prefix length of the network segment of Docker. After you configure an IPv6 network segment address, IPv6 address is supported in the container.

Notes:

- To ensure that Docker can be used as expected, you need to enter an IPv4 network segment address in the **IP/Netmask** field.
- The specified network segment address cannot overlap with the interface address within trust-vr.

Warning Page Management

Warning page management includes picture management and page management of user-defined warning pages.

Related links:

- Configuring URL Filtering Objects -Warning Page
- Configuring Content Filtering Objects - Warning Page

Page Management

You can upload the required pictures and reference the picture in the user-defined warning page as needed. In the picture management page, the name , previews and the last modification time of uploaded picture will be displayed in a list.

Uploading the Picture

To upload the picture, take the following steps:

1. Select **System** > **Warning Page Management** > **Picture Management**.
2. Click **New** to open the **Upload Picture Configuration** dialog.



3. Type the name of the user-defined picture into the **Name** box.
4. Click **Upload Picture** and select the local picture file to be uploaded.

5. After uploading, the picture will be previewed in the dialog.

6. Click **OK** to save the configuration.

> **Notes:** Only the following types of pictures can be uploaded: jpeg, jpg, png, gif, jfif; the size of uploaded pictures is limited to 24KB; the system allows up to 32 picture files to be uploaded.

Editing the Picture

To replace and modify the uploaded picture, take the following steps:

1. Select **System** > **Warning Page Management** > **Picture Management**.

2. Select the check box of the picture to be edited in the list and click the **Edit**.

3. In the **Upload Picture Configuration** dialog, click the **Upload Picture** button to upload the picture file.

4. Click **OK** to save the configuration.

Deleting the Picture

To delete the picture, take the following steps:

1. Select **System** > **Warning Page Management** > **Picture Management**.

2. Select the check box of the picture to be deleted in the list and click the **Delete**.

3. In the delete confirmation dialog, click the **Yes** button to complete the deletion.

> **Notes:** Before deleting the picture, please make sure that the picture is not referenced by the user-defined warning page, otherwise it cannot be deleted.

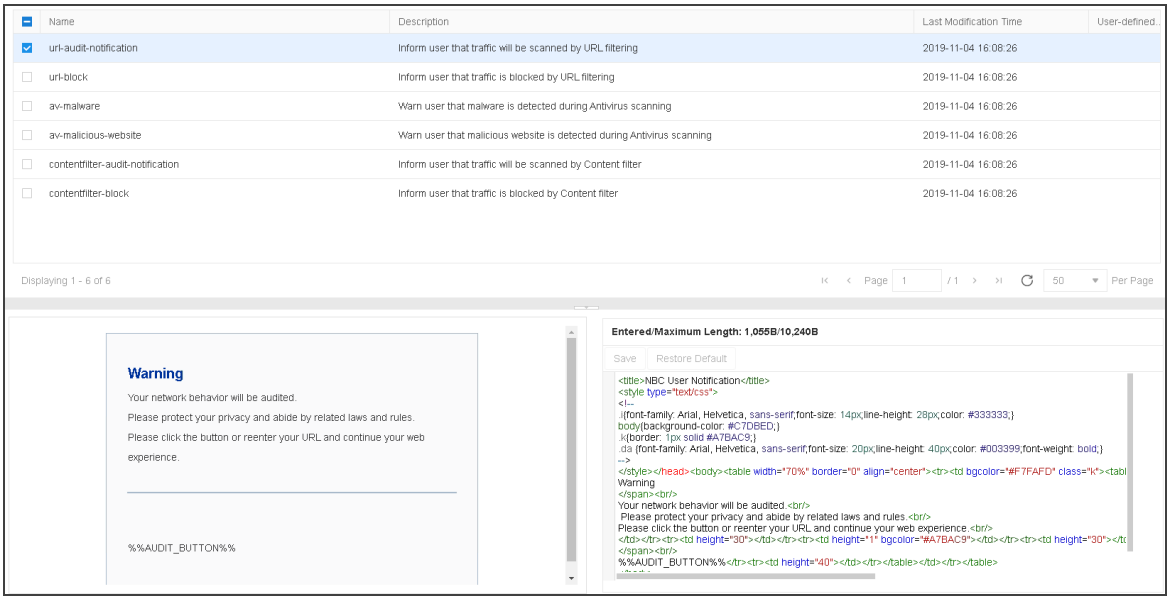
Page Management

System supports 6 types of user-defined warning pages, and the user-defined warning page already contains the reference string and warning information content displayed by default. You can add or modify the reference string by using html encoding to customize the warning message text, pictures and other content.

- url-adudit-notification: Inform user that traffic will be scanned by URL filtering.
- url-block: Inform user that traffic is blocked by URL filtering.
- av- malware: Warn user that malware is detected during Antivirus scanning.
- av-malicious-website: Warn user that malicious website is detected during Antivirus scanning.
- ontentfilter-audit-notification: Inform user that traffic will be scanned by Content filter.
- contentfilter-block: Inform user that traffic is blocked by Content filter.

To configure the user-defined warning page, take the following steps:

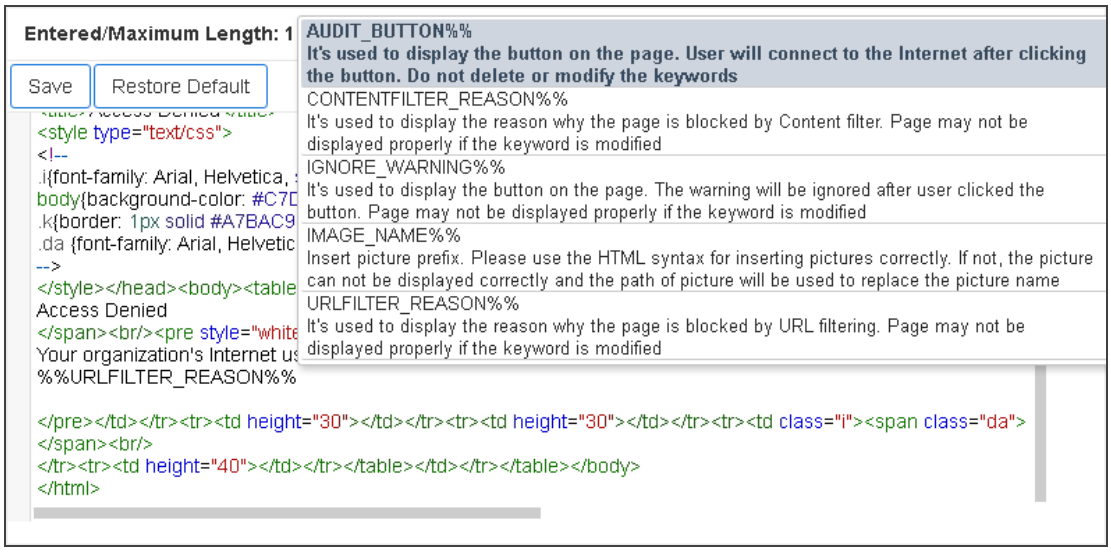
1. Select **System** > **Warning Page Management** > **Page Management**.



In the Page Management page, view the details of user-defined warning page.

- The list at the top of the page shows the name, description, last modification time and the enable status of 6 types of user-defined warning pages supported by system.
- In the lower left part of the page, a page preview showing the selected user-defined warning page.
- In the lower right part of the page, the default html encoding of the user-defined warning page is displayed, and you can use the html encoding method to customize the page content in this part.

2. In the list above, select the check box of the warning page that needs to be customized.
3. In the html encoding page below, modify the content of the warning message, or enter "%%" to select the reference string to be added and reference the corresponding content or picture.



User-defined warning page can contain the following reference strings.

Reference String	Description
%%AUDIT_BUTTON%%	It's used to display a button on the page. When you click the button, you can connect to the Internet.

Reference String	Description
	Note: This reference string is required in the "url-adudit-notification" and "contentfilter-audit-notification" pages. Please do not delete or modify this keyword.
%%IGNORE_ WARNING%%	It is used to display a button on the page. You can click the button to ignore the prompt and continue browsing. **Note**: This reference string is the default reference string displayed on the page. After modification, it may cause ignore prompts and buttons to be displayed normally.
%%IMAGE_NAME%%	Picture prefix, which is used to reference a picture uploaded in Picture Management, and output the picture on the user-defined warning page.
%%URLFILTER_ REASON%%	It's used to display the reason for URL filtering blocking on the "url-block" page. **Note**: This reference string is the default reference string displayed on the page. After modification, the reason may not be displayed normally.
%%VIRUS_NAME%%	It's used to display the virus name on the "av- malware" page. **Note**:This reference string is the default reference string displayed on the page. After modification, the virus name may not be displayed normally.

Reference String	Description
%%CONTENTFILTER_REASON%%	It's used to display the reason for content filtering blocking on the "contentfilter-block" page. **Note:** This reference string is the default reference string displayed on the page. After modification, the reason may not be displayed normally.

4. After modifying the html encoding, click **Save** to save the configuration. At the same time, the user-defined warning page will be enabled, and will be displayed in the "User-defined" column of the upper list.

5. If you need to restore the default content of the cuser-defined warning page, click the **Restore Default**.

SNMP

The device is designed with a SNMP Agent, which can receive the operation request from the Network Management System and give the corresponding information of the network and the device.

The device supports SNMPv1 protocol, SNMPv2 protocol and SNMPv3 protocol. SNMPv1 protocol and SNMPv2 protocol use community-based authentication to limit the Network Management System to get device information. SNMPv3 protocol introduces an user-based security module for information security and a view-based access control module for access control.

The device supports all relevant Management Information Base II (MIB II) groups defined in RFC-1213, the Interfaces Group MIB (IF-MIB) using SMIv2 defined in RFC-2233, the User-based Security Model (USM) for version 3 defined in RFC-2574 and the View-based Access Control Model (VACM) defined in RFC-2575. Besides, the system offers a private MIB, which contains the system information, IPSec VPN information and statistics information of the device. You can use the private MIB by loading it into an SNMP MIB browser on the management host.

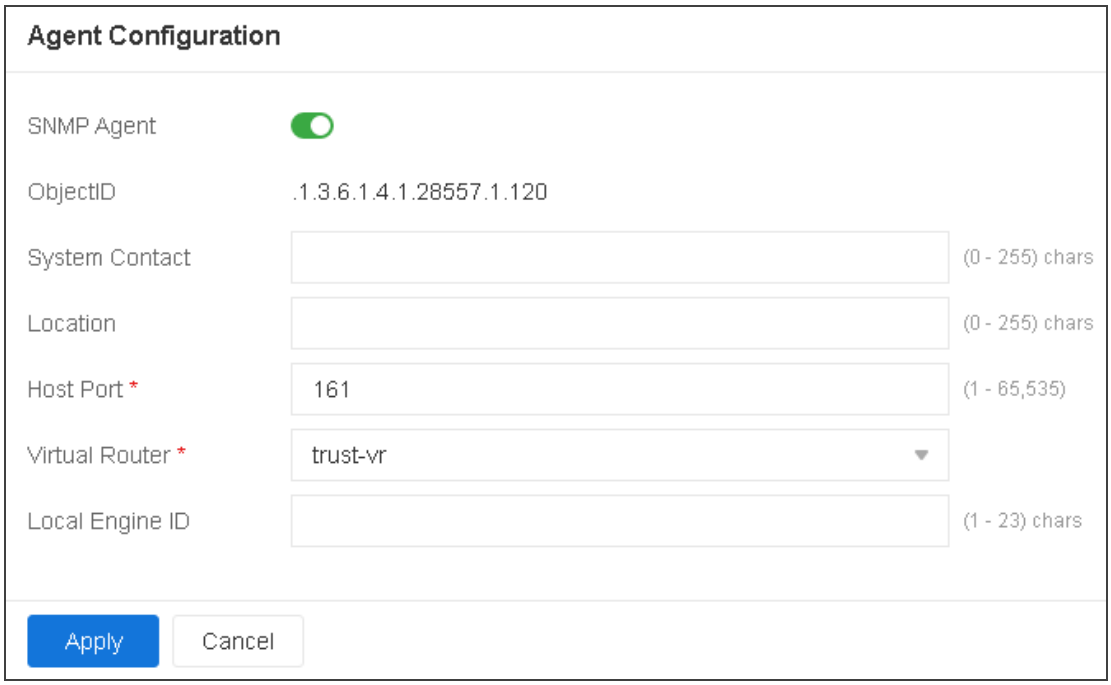
SNMP Agent

The device is designed with a SNMP Agent, which provides network management and monitors the running status of the network and devices by viewing statistics and receiving notification of important system events.

To configure an SNMP Agent, take the following steps:

1. Select **System** > **SNMP** > **SNMP Agent**.

2. Click **Enable** button. In the SNMP Agent page, configure these values.



Option	Description
SNMP Agent	Select the **Enable** check box for Service to enable the SNMP Agent function.
ObjectID	The Object ID displays the SNMP object ID of the system. The object ID is specific to an individual system and cannot be modified.

Option	Description
System Contact	Type the SNMP system contact information of the device into the **System Contact** box. System contact is a management variable of the group system in MIB II and it contains the ID and contact of relevant administrator of the managed device. By configuring this parameter, you can save the important information to the device for the possible use in case of emergency.
Location	Type the location of the device into the **Location** box.
Host Port	Type the port number of the managed device into the **Host Port** box.
Virtual Router	Select the VRouter from the **Virtual Router** drop-down list.
Local EnginelID	Type the SNMP engine ID into the **Local EngineID** box. When the **Local EngineID** parameter is left empty, the HA master and backup devices generate a default engine ID respectively, which is different from each other.

3. Click **Apply**.



Notes: SNMP Engine ID identifies an engine uniquely. SNMP Engine is an important component of the SNMP entity (Network Management System or managed network device) which implements the functions like the reception/sending and verification of SNMP messages, PDU abstraction, encapsulation, and communications with SNMP applications.

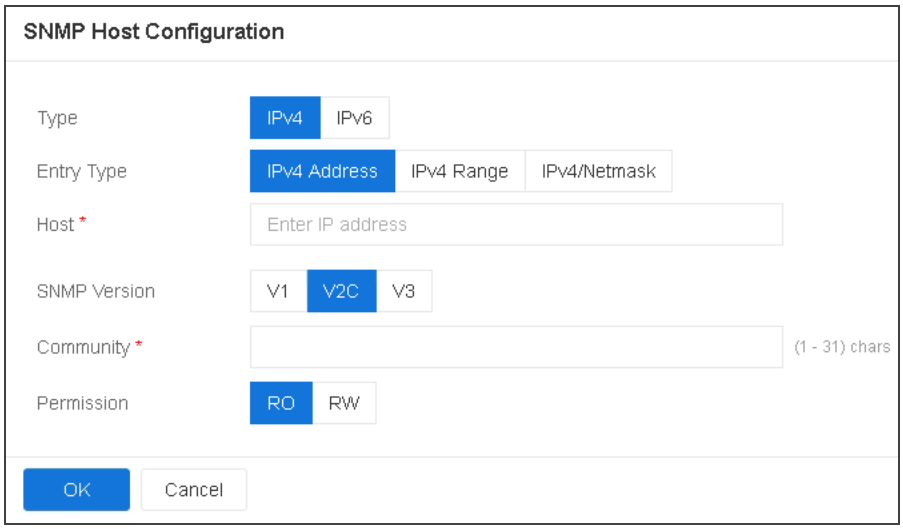
SNMP Host

To create an SNMP host, take the following steps:

1. Select **System** > **SNMP** > **SNMP Host**.

2. Click **New**.

3. In the SNMP Agent dialog box, configure these values.



Option	Description
Type	Select the SNMP host type: **IPv4** or **IPv6**. This configuration is only suitable for IPv6 system version.

Entry Type	You can configure IPv4-typed SNMP host or IPv6-typed SNMP host.
	• When the **Type** is selected as IPv4, specify **IPv4 Address**, **IPv4 Range**, and **IPv4/Netmask**:
	  • IPv4 Address: Type the IPv4 address of the host in the **Host** box.
	  • IPv4 Range: Type the start IPv4 address and the end IPv4 address in the **Host** box.
	  • IPv4/Netmask: Type the IPv4 address and the net-mask of the host in the **Host** box.

Option	Description

	• When the **Type** is selected as IPv6, specify **IPv6 Address**, **IPv6 Range**, and **IPv6/Prefix**:
	  • IPv6 Address: Type the Ipv6 address of the host in the **Host** box.
	  • IPv6 Range: Type the start Ipv6 address and the end Ipv6 address in the **Host** box.
	  • IPv6/Prefix: Type the Ipv6 address and the prefix length of the host in the **Host** box.

SNMP Version	Select the SNMP version from the **SNMP Version** drop-down list.
Community	Type the community for the SNMP host into the **Community** box. Community is a password sent in clear text between the manager and the agent. This option is only effective if the SNMP version is V1 or V2C.

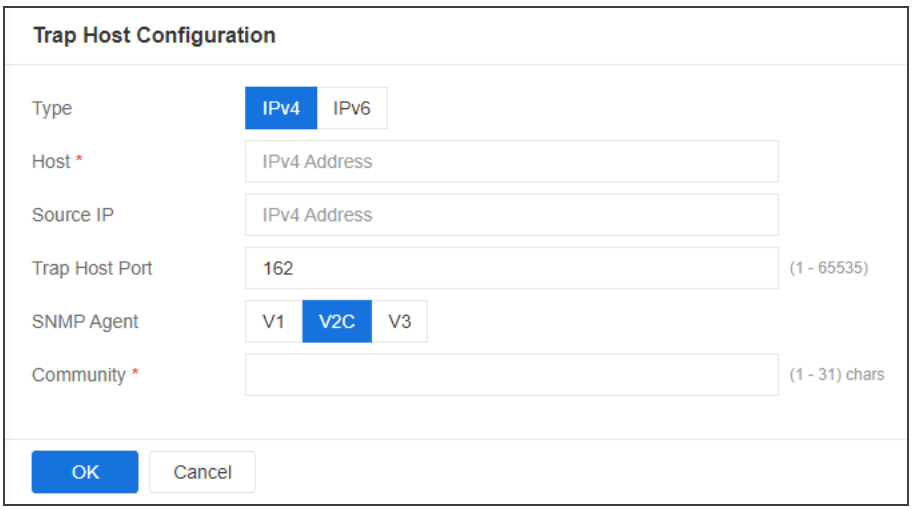
Permission	Select the read and write permission for the community from the Permission drop-down list. This option is only effective if the SNMP version is V1 or V2C.
	  • RO: Stand for read-only, the read-only community is only allowed to read the MIB information.
	  • RW: Stand for read-write, the read-write community is allowed to read and modify the MIB information.

4. Click **OK**.

Trap Host

To create a Trap host, take the following steps:

1. Select **System** > **SNMP** > **Trap Host**.
2. Click **New**.
3. In the Trap Host Configuration dialog box, configure these values.



Option	Description
Type	Select the type : IPv4 or IPv6. This configuration is only suitable for IPv6 system version.
Host	When the **Type** is selected as IPv4, type the IPv4 address of the host in the **Host** box. When the **Type** is selected as IPv6, type the IPv6 address of the host in the **Host** box.
Source IP	When the **Type** is selected as IPv4, type the IPv4 address of the source IP address that sends SNMP trap packets in the **Source IP** box. When the **Type** is selected as IPv6, type the IPv4 address of the source IP address that sends SNMP trap packets

Option	Description
	in the **Source IP** box. Note: In the HA environment, the source IP address that sends SNMP trap packets configured on the master device will not be synchronized with the backup device.
Trap Host Port	Type the port number for the Trap host into the **Trap Host Port** box.
SNMP Agent	Select the SNMP version from the **SNMP Agent** drop-down list. • V1 or V2C: Type the community for the Trap host into the **Community** box. • V3: Select the V3 user from the **V3 User** drop-down list. Type the Engine ID for the trap host into the **Engine ID** box.

4. Click **OK**.

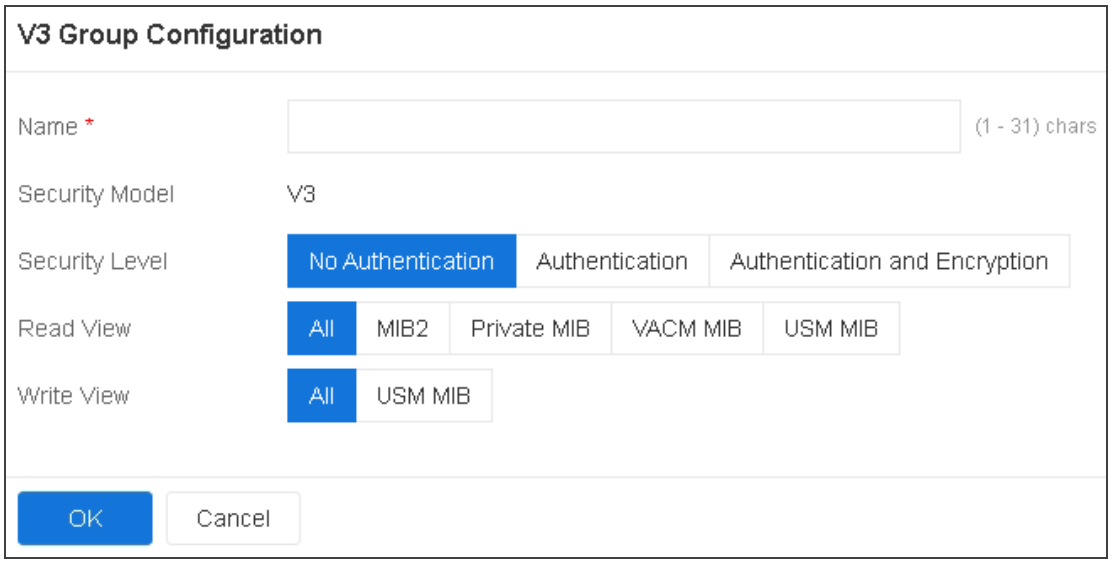
V3 User Group

SNMPv3 protocol introduces a user-based security module. You need to create an SNMP V3 user group for the SNMP host if the SNMP version is V3.

To create a V3 user group:

1. Select **System** > **SNMP** > **V3 User Group**.
2. Click **New**.

3. In the V3 Group Configuration dialog box, enter values.



Option	Description
Name	Type the SNMP V3 user group name into the **Name** box.
Security Model	The Security model option displays the security model for the SNMP V3 user group.
Security Level	Select the security level for the user group from the **Security Level** drop-down list. Security level determines the security mechanism used in processing an SNMP packet. Security levels for V3 user groups include **No Authentication** (no authentication and encryption), **Authentication** (authentication algorithm based on MD5 or SHA) and **Authentication and Encryption** (authentication algorithm based on MD5 or SHA and message encryption based on AES and DES).
Read View	Select the read-only MIB view name for the user group: • All: The user group can read all MIB views.

Option	Description
	• MIB2: The user group can read the public MIB (MIB-II) defined in RFC-1213 and RFC-2233. • Private MIB: The user group can read Hillstone Networks private MIB. • VACM MIB: The user group can read the View-based Access Control Model (VACM) MIB defined in RFC-2575. • USM MIB: The user group can read the User-based Security Model (USM) MIB for version 3 defined in RFC-2574.
Write View	Select the write MIB view name for the user group: • All: The user group can modify all MIB views (USM MIB). • USM MIB: The user group can modify the User-based Security Model (USM) MIB for version 3 defined in RFC-2574.

4. Click **OK**.

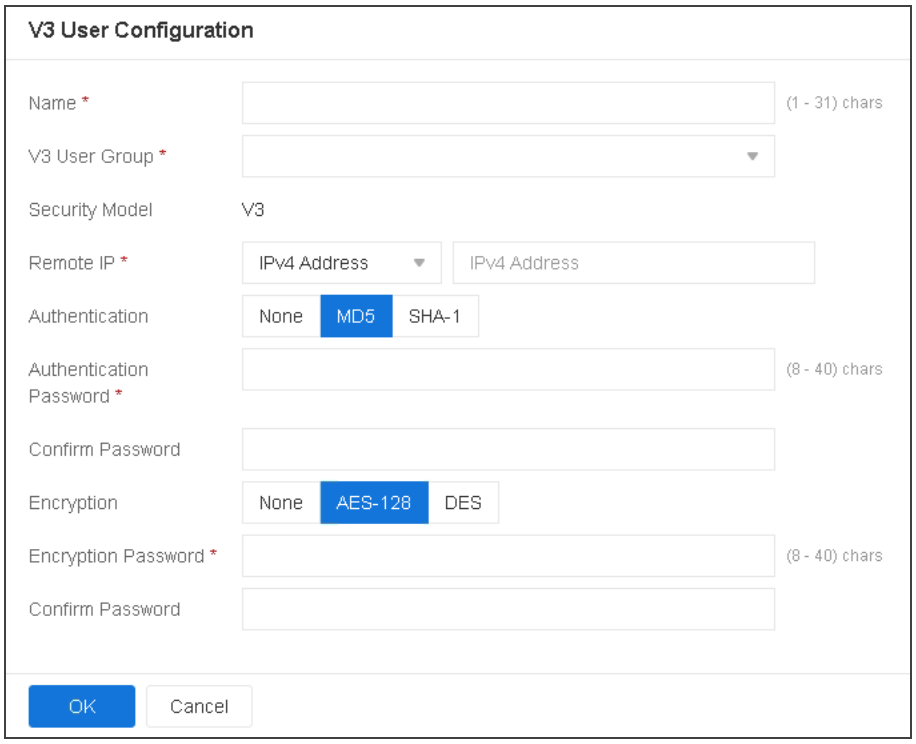
V3 User

If the selected SNMP version is V3, you need to create an SNMP V3 user group for the SNMP host and then add users to the user group.

To create a user for an existing V3 user group, take the following steps:

1. Select **System** > **SNMP** > **V3 User**.
2. Click **New**.

3. In the V3 User Configuration dialog box, configure these values.



Option	Description
Name	Type the SNMP V3 user name into the **Name** box.
V3 User Group	Select an existing user group for the user from the Group drop-down list.
Security Model	The Security model option displays the security model for the SNMP V3 user.
Remote IP	Type the IP address of the remote management host into the **Remote IP** box. When system version is IPv4, this IP address can be an IPv4 address or IPv4/Netmask. When system version is IPv6, this IP address can be an IPv4 address, IPv4/Netmask, IPv6 address, or IPv6/Prefix.

Option	Description
Authentication	Select the authentication protocol from the **Authentication** drop-down list. By default, this parameter is None, i.e., no authentication.
Authentication Password	Type the authentication password into the **Authentication password** box.
Confirm Password	Re-type the authentication password into the **Confirm Password** box to confirm.
Encryption	Select the encryption protocol from the **Encryption** drop-down list.
Encryption Password	Type the encryption password into the **Encryption Password** box.
Confirm Password	Re-type the encryption password into the **Confirm Password** box to confirm.

4. Click **OK**.

Downloading MIB Files

To download MIB files to your PC, take the following steps:

1. Select **System** > **SNMP** > **MIB File**.
2. Click **Download**.

SNMP Server

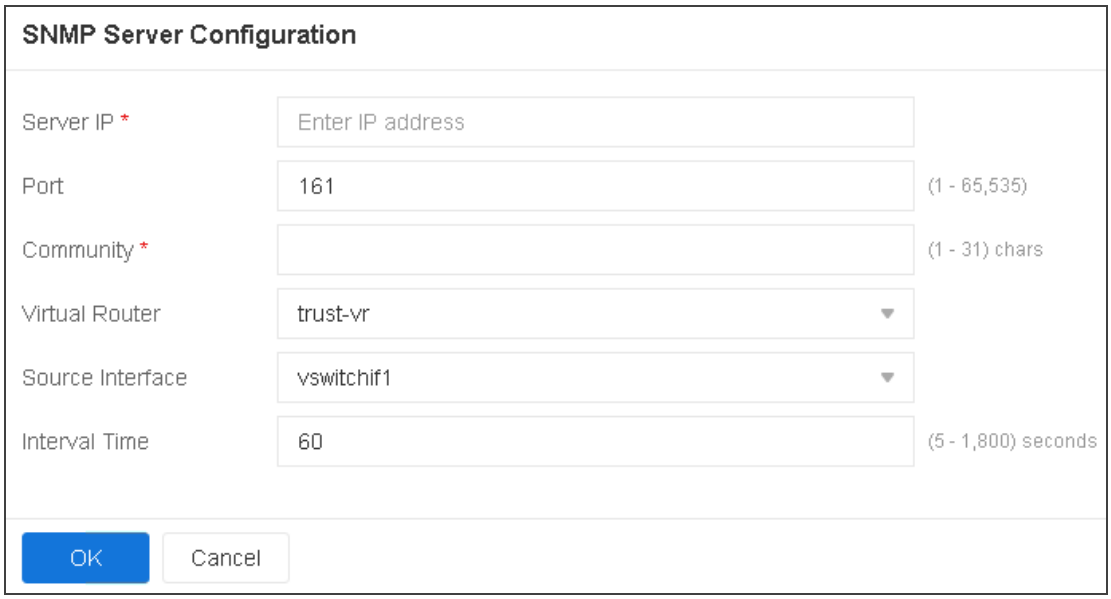
You can configure the SNMP server to get the ARP information through the SNMP protocol.

Creating an SNMP Server

To create an SNMP server, take the following steps:

1. Select **System** > **SNMP server**.

2. Click **New**.



Option	Description
Server IP	Type the SNMP server IP address into the **Server IP** box.
Port	Type the port number for the SNMP server into the **Port** box. The value range is 1 to 65535, the default value is 161.
Community	Type the community for the SNMP server into the **Community** box. This option is only effective if the SNMP version is V1 or V2C.
Virtual Router	Select the VRouter from the drop-down list.
Source Interface	Select the source interface from the drop-down list for receiving ARP information on the SNMP server.
Interval Time	Type the the interval into the **Interval Time** box for receiving ARP information on the SNMP server. The value range

Option	Description
	is 5 to 1800 seconds, the default value is 60 seconds.

3. Click **OK**.

NETCONF

Network Configuration Protocol (NETCONF) provides a mechanism for managing network devices. You can add, modify, and delete configurations of network devices, and obtain configuration and status information of network devices. Through NETCONF, network devices provide standard application programming interfaces (API). Applications can directly use these application programming interfaces to send and obtain configurations from network devices.

Comparison between NETCONF and SNMP:

Function	SNMP	NETCONF
Configuration management	SNMP does not provide a locking mechanism.	NETCONF provides a locking mechanism to avoid configuration conflicts arising from multi-user operations.
Inquiry	You can inquire about one or more nodes of the table through multiple interactions with the system.	You can inquire about all configurations of the system.
Extensibility	Poor extensibility	Good extensibility. NETCONF adopts a layered architecture and each layer is independent. Therefore, the impact on the upper-layer protocol will be minimalized when you extend a layer of NETCONF. Also, NETCONF adopts the XML, which allows the protocol to be extensible in terms of management ability and sys-

Function	SNMP	NETCONF
		tem compatibility.
Security	Take the latest SNMPv3 as an example. SNMPv3 only provides the user-based security module and cannot be added to other security modules.	NETCONF exploits current security protocols to provide security protection. It is not bound to a specific security protocol. Therefore, in practice, NETCONF is more flexible than SNMP. **Note:** SSH is the priority at the NETCONF transport layer. XML message is carried by SSH protocol.

Through the NETCONF client, you can modify the configuration of Hillstone devices and obtain configuration and status information. You can configure the following function modules:

- Object module: You can create/delete/edit address book and host book through the NETCONF client.
- Network module: You can create/delete/edit zone, interface, DNS server, DNS proxy, DHCP, destination route, source route, policy route, OSPF, BGP, IPsec VPN, and SSL VPN through the NETCONF client.
- Policy module: You can create/delete/edit a policy, SNAT, and DNAT through the NETCONF client.



Notes:

- NETCONF function requires you to configure the login type of administrators and the trusted host as NETCONF, and the management method of interfaces as NETCONF. It is recommended to configure the three options before you enable NETCONF.



- When the root VSYS enables NETCONF, you can configure the login type of non-root administrators as NETCONF to enable NETCONF on non-root VSYS.

Configuring the NETCONF Agent

The StoneOS system is equipped with a NETCONF agent, which manages the configuration of the device.

You can configure the NETCONF agent only by CLI. For more information, refer to the chapter on **Network Configuration Protocol (NETCONF)** of the **StoneOS CLI User Guide**.

Configuring NETCONF Candidate

NETCONF candidate enables you to modify the configuration of the current device but apply the modification later so that the current service traffic is not influenced. You can modify the configuration of the candidate, and replace the current configuration with the candidate configuration according to your own needs. The replacement takes effect immediately. By default, the NETCONF candidate is disabled.

You can configure the NETCONF candidate only by CLI. For more information, refer to the chapter on **Network Configuration Protocol (NETCONF)** of the **StoneOS CLI User Guide**.

Configuring NETCONF Timeout

You can perform operations such as offering configuration to a Hillstone device through the NETCONF client. If you do not perform any operations on the NETCONF client for a certain amount of time, you will be required to log in again to perform subsequent operations. By default, the timeout period is 10 minutes.

You can configure NETCONF timeout only by CLI. For more information, refer to the chapter on **Network Configuration Protocol (NETCONF)** of the **StoneOS CLI User Guide**.

Extended Services

System supports to connect to other Hillstone products to provide more services. Currently, the extended services include connecting Hillstone Security Management (HSM) and CloudPano (NFV Management System) . For specific configurations, refer to one of the following topics:

- Connecting to Centralized Management

Connecting to Centralized Management

System supports to connect to other Hillstone products, include connecting to HSM and CloudPano.

Connecting to HSM

Hillstone Security Management (HSM) is a centralized management platform to manage and control multiple Hillstone devices. Using WEB2.0 and RIA (Rich Internet Application) technology, HSM supports visualized interface to centrally manage policies, monitor devices, and generates reports.

Each firewall system has an HSM module inside it. When the firewall is configured with correct HSM parameters, it can connect to HSM and be managed by HSM.

In addition, firewall can also send the following information to HSM:

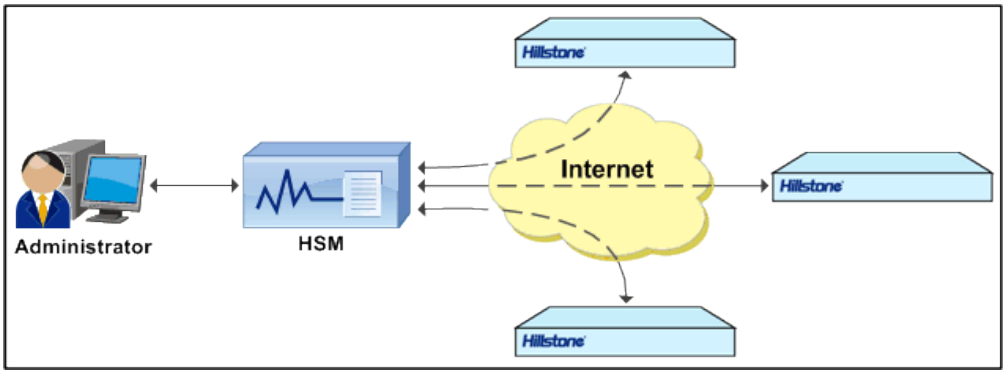
- Interface information, including latency, jitter, packet loss rate, etc.
- Application data information on the interface, including application latency, jitter, upstream and downstream packet loss rate, etc.

Notes: For more information about HSM, please refer to HSM User Guide.

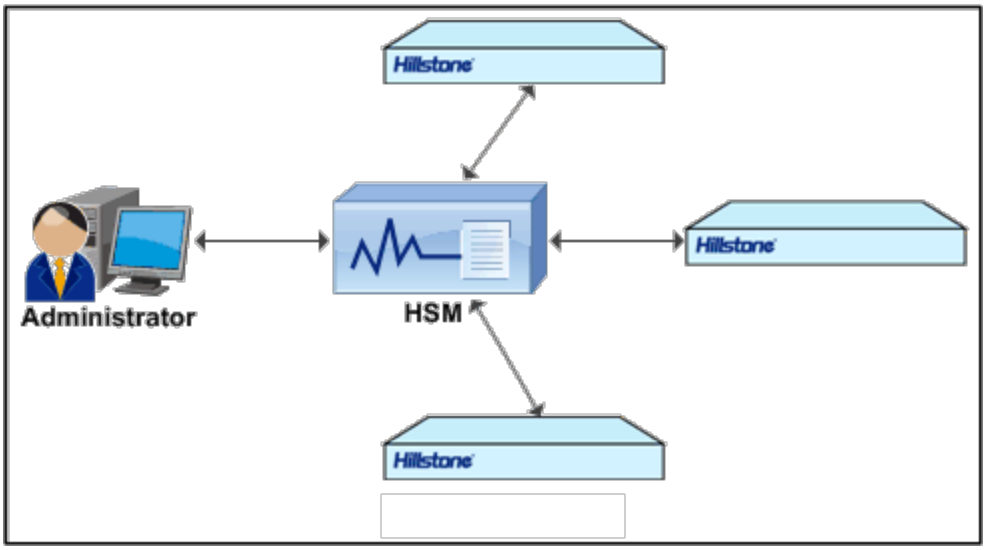
HSM Deployment Scenarios

HSM normally is deployed in one of the two scenarios: installed in public network or in private network:

- Installed in public network: HSM is remotely deployed and connected to managed devices via Internet. When the HSM and managed devices have a accessible route, the HSM can control the devices.



- Installed in private network: In this scenario, HSM and the managed devices are in the same subnet. HSM can manage devices in the private network.



Connecting to CloudPano

CloudPano (NFV Management System) is deployed on the cloud platform as a cloud host. It provides an integrated service among firewall, cloud platform and SDN. It can also manage the life-cycle of VNF and check whether configurations of VNF are consistent with that on the cloud platform.

After the server IP/domain name and port of the CloudPano are correctly configured on the device, the device can be connected to the CloudPano, and the CloudPano can manage and control the device. If the connection is disconnected for a period of time, all configurations cannot be delivered.

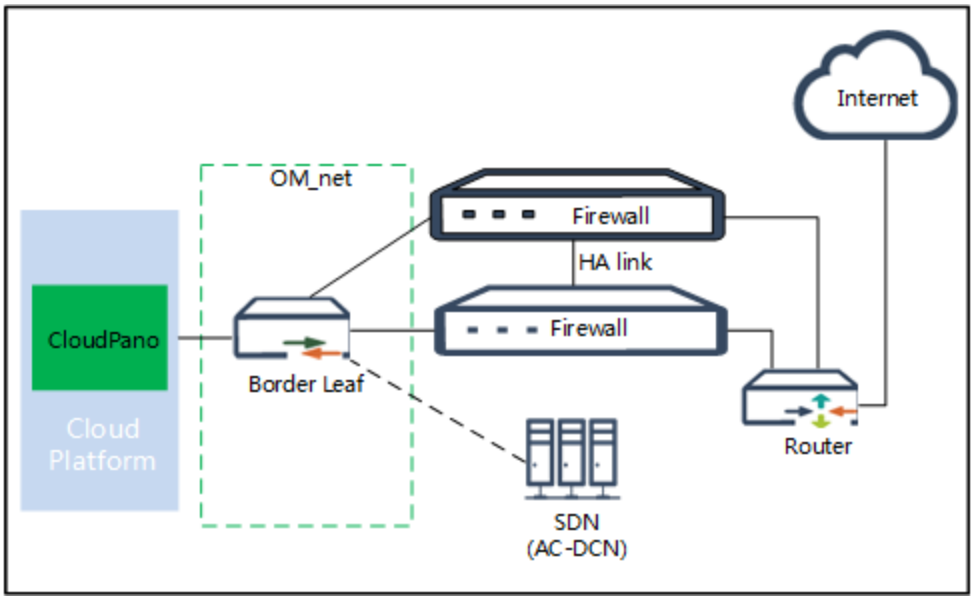


Notes: All platforms support the registration of the CloudPano, but the CloudPano can manage only certain types of devices. If the CloudPano does not support management, the configuration may not be delivered properly. For details about the devices that can be managed by the CloudPano, see the *CloudPano WebUI User Guide*.

CloudPano Deployment Scenarios

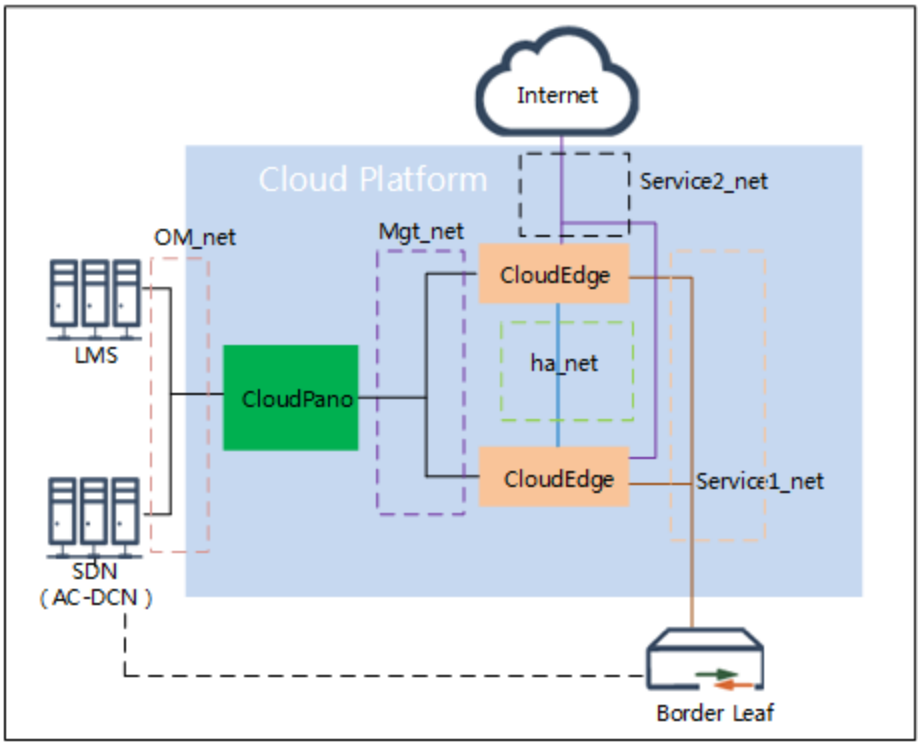
CloudPano provides two deployment typologies, including selecting hardware firewall or virtual firewall.

- The deployment typology of hardware firewall: After the hardware firewall is deployed, CloudPano will be deployed as the cloud host on the Compute node of the cloud platform. It will also be connected with the SDN controller and two HA firewall devices via the OM_net. When you create a router via the cloud platform WebUI, CloudPano will create VSYS on the hardware firewall automatically to protect the network of the router.



- The deployment typology of the virtual firewall: After the deployment, CloudPano will be deployed as the cloud host on the Compute node of the cloud platform. It will be connected with the LMS server and SDN controller via the OM_net, and be connected with the MGT interface via the Mgt_net. The Border Leaf will connect to the Service1_net of CloudEdge at the same time. When you create a route on the cloud platform, CloudPano will create an HA

environment of the virtual firewall automatically to protect the network of the router.



Connecting to Centralized Management

To configure HSM or CloudPano parameters in the firewall, take the following steps:

1. Select **System > Extended Services > Connecting to Centralized Management**.Click **Edit** button.

2. Click **Enable** button of HSM/CloudPano Agent field to enable this feature.



3. Input HSM/CloudPano server's IP address in the Sever IP/Domain text box. The address cannot be 0.0.0.0 or 255.255.255.255, or mutlicast address.
4. Enter the port number of HSM/CloudPano server.
5. Click **OK**.



Notes: The Syslog Server part shows the HSM/CloudPano server's syslog server and its port.

Connecting to Hillstone Cloud Service Platform

Hillstone Cloud Service Platform is a cloud security services platform, which provides cloud services including CloudView, Cloud Sandbox and CloudVista (Threat Intelligence Center). Hillstone Cloud Service is the cloud capability center of Hillstone and the brain of the cloud-network integration. After the service is enabled, your device will be connected with the Hillstone cloud, which will provide you with a wider range of threat intelligence, improve the protection capability of your device, and enable you to carry out real-time monitoring, inspection and report acquisition of the device and traffic on the cloud anytime and anywhere. These Hillstone cloud applications can greatly enhance the security, visibility, and usability of networks.

- CloudView: CloudView is a SaaS product. It is deployed on the public cloud to provide users with online on-demand services. Hillstone devices register with the cloud service platform and upload device information, traffic data, threat events, system logs and so on to the cloud service platform, and the visual display is provided by CloudView . Users can monitor the device status, gain reports and threat analysis through the Web or mobile phone APP. In addition, you can also use CloudView to send configuration to the device. For more information about CloudView, refer to the *CloudView FAQs*.
- Cloud Sandbox: It is a technology adopted by the Sandbox function. After a suspicious file being uploaded to the Hillstone cloud service platform, the cloud sandbox will collect behaviors of the file, analyze the collected data, verify the legality of the file, send the analysis

result to system and deal with the malicious file according to the actions set by system. For specific configurations of cloud sandbox, refer to **Threat Prevention > Sandbox**.

- CloudVista (Threat Intelligence Center): Threat Intelligence function can upload some elements in the logs generated by each module to the cloud service platform, such as IP address, domain, etc. The cloud service platform will check whether the elements have threat intelligence through the threat center. You can view threat intelligence information related to elements through the threat intelligence center.

Configurations about Connecting to Hillstone Cloud Service Platform

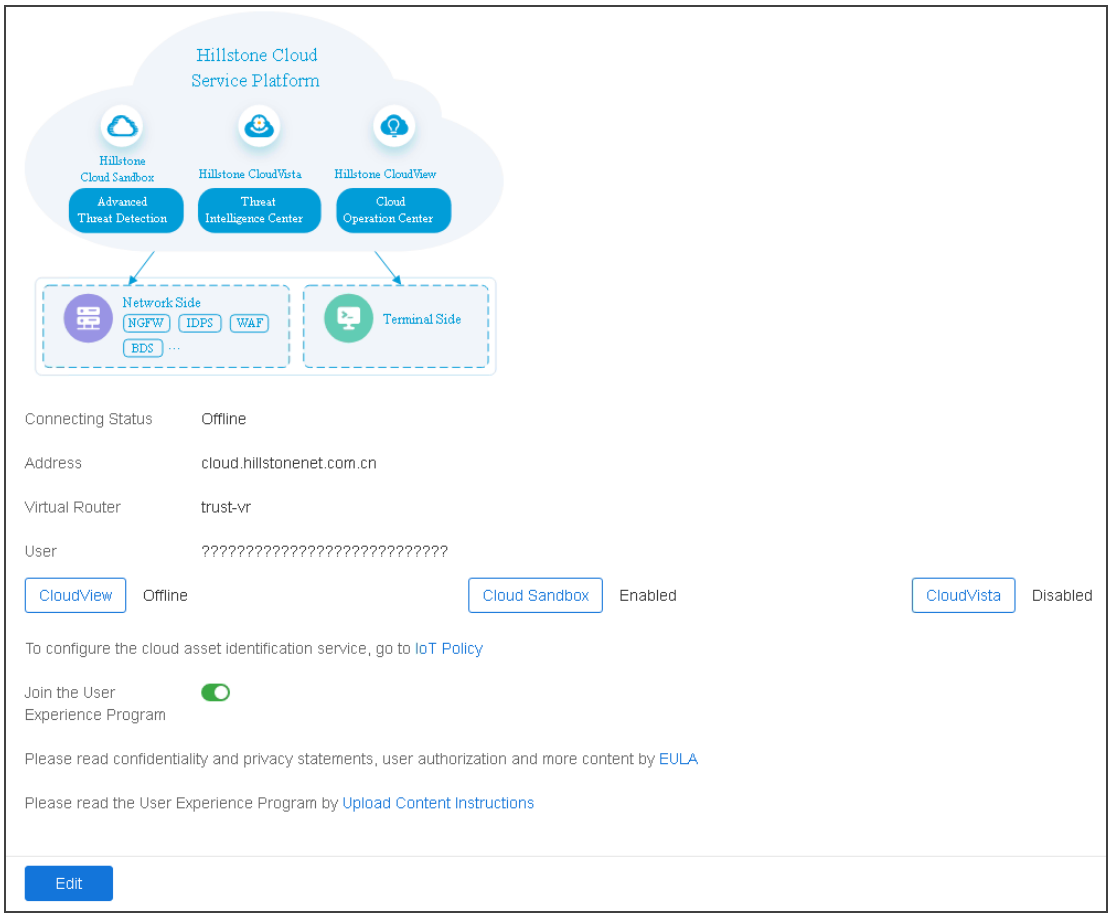
The configurations of Hillstone Cloud Service Platform include:

- Connecting to Hillstone Cloud Service Platform
- Configuring CloudView
- Configuring Cloud Sandbox
- Configuring CloudVista
- Enabling Hillstone Cloud Service with One Click

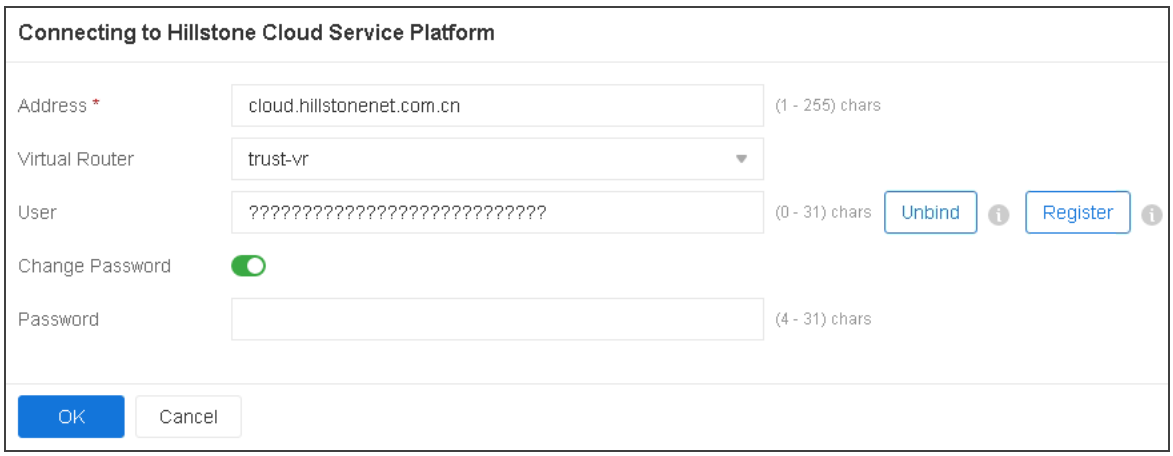
Connecting to Hillstone Cloud Service Platform

To connect to the Hillstone Cloud Service Platform, take the following steps:

1. Select **System > Connecting to Hillstone Cloud Service Platform**.



2. At the lower-left corner, click the **Edit** button. The Hillstone Cloud Service Platform configuration page appears.



Option	Description
Address	Enter the IPv4 address, IPv6 address, or URL of domain name of the cloud service platform. The default value is cloud.hillstonenet.com.cn.
Virtual Router	Select the VRouter of the Cloud service platform from the drop-down list.
User	Enter the username of the cloud service platform and bind the device with this account. Click the **Register** button and sign up for an account on the Hillstone cloud service login page. Click **Unbind** to remove the binding relationship between the device and the account.
Password	Enter the password of the user.
Change Password	When you edit the configuration of the cloud platform, you can see the Change Password function. After you enable this function, the password field is displayed. To change the password, enter a new password in this field and click **OK**.

3. Click **OK**.
4. Click the **Enable** button next to **Join the User Experience Program**. This function will upload the threat prevention data to the cloud service platform. The uploaded data will be used for internal research to reduce the false positives and improve the protection capability of your device.
5. Click **EULA** to read confidentiality and privacy statements, user authorizations and other content.
6. Click **Upload Content Instructions** to view the content of user experience program.

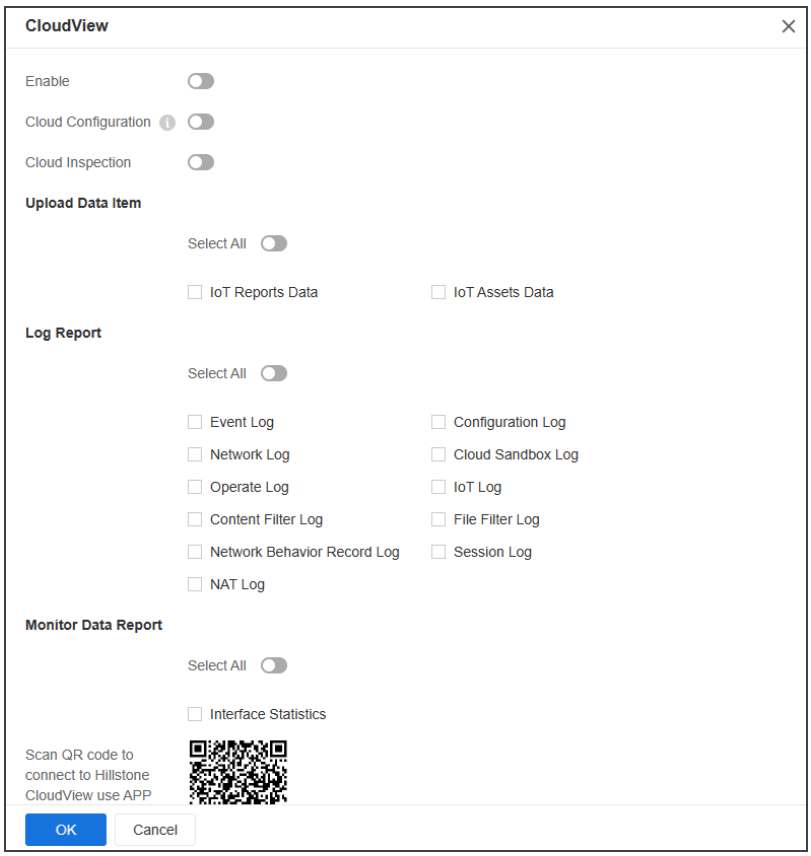
Configuring CloudView

CloudView can be used to visualize device information, traffic data, threat events, and system logs that are uploaded to the cloud platform.

To configure CloudView, take the following steps:

1. Select **System > Connecting to Hillstone Cloud Service Platform**.

2. Click **CloudView**.



3. In this panel, configure the following options.

Option	Description
Enable	Click the **Enable** button to enable the Hillstone CloudView service.
Cloud Con-	You can configure this function only when CloudView is

Option	Description
figuration	enabled. Click the enable button to allow CloudView to send configuration to the device. The system will load the real-time configuration sent by CloudView. • PTF Dynamic IP Blacklist: Log in to CloudView to send the configuration of the PTF dynamic IP blacklist to the root VSYS of the device. Both IPv4 and IPv6 addresses are supported. You can also specify the virtual router to take effect as well as the block duration. When the system receives the configuration task from CloucView, corresponding dynamic IP blacklist entries, configuration logs, and operation logs are generated.
Cloud Inspection	Click the **Enable** button to enable the cloud inspection function and upload the collected inspection data to the cloud service platform. With the cloud inspection function, the device can receive and execute the inspection instructions from the cloud, and upload the collected inspection data to the cloud service platform, which enables you to carry out real-time monitoring and management on the cloud anytime and anywhere.
Upload Data Item	Select the data item that you want to upload to the cloud platform, including the IoT reports data, and IoT Assets data. If you enable Select All, all IoT data are uploaded.
Log Report	Select the type of logs that you want to upload to the cloud platform, including event logs, threat logs, configuration logs, network logs, cloud sandbox logs, operation logs, content filter

Option	Description
	logs, file filter logs, network behavior record logs, session logs, and NAT logs. If you enable Select All, all logs are uploaded. Note: • The advanced edition of CloudView allows you to view all types of logs that are uploaded. If you use the basic edition of CloudView, you can only view uploaded event logs and threat logs on the CloudView.
Monitor Data Report	Select the monitor data type that you want to upload to the cloud platform, including the traffic ranking, session ranking, URL ranking, device information, VPN statistics, and interface statistics (including the maximum upstream rate, maximum downstream rate, average upstream rate, and average down-stream rate of each interface in the device). If you enable Select All, all monitor data is uploaded.
Scan QR code to connect to Hillstone CloudView use APP	Scan the QR code using a QR reader app on your smartphone or mobile device to connect to Hillstone CloudView via APP.
Visit CloudView	Click the button to visit CloudView.

4. Click **OK**.

Configuring Cloud Sandbox

Cloud Sandbox can be used to identify malicious files and their risk levels via file analysis.

To configure Cloud Sandbox, take the following steps:

1. Select **System > Connecting to Hillstone Cloud Service Platform**.
2. Click **Cloud Sandbox**.
    - Click **Sandbox** to configure the sandbox function on the **Profile** page. For more information, see Threat Prevention > Sandbox.

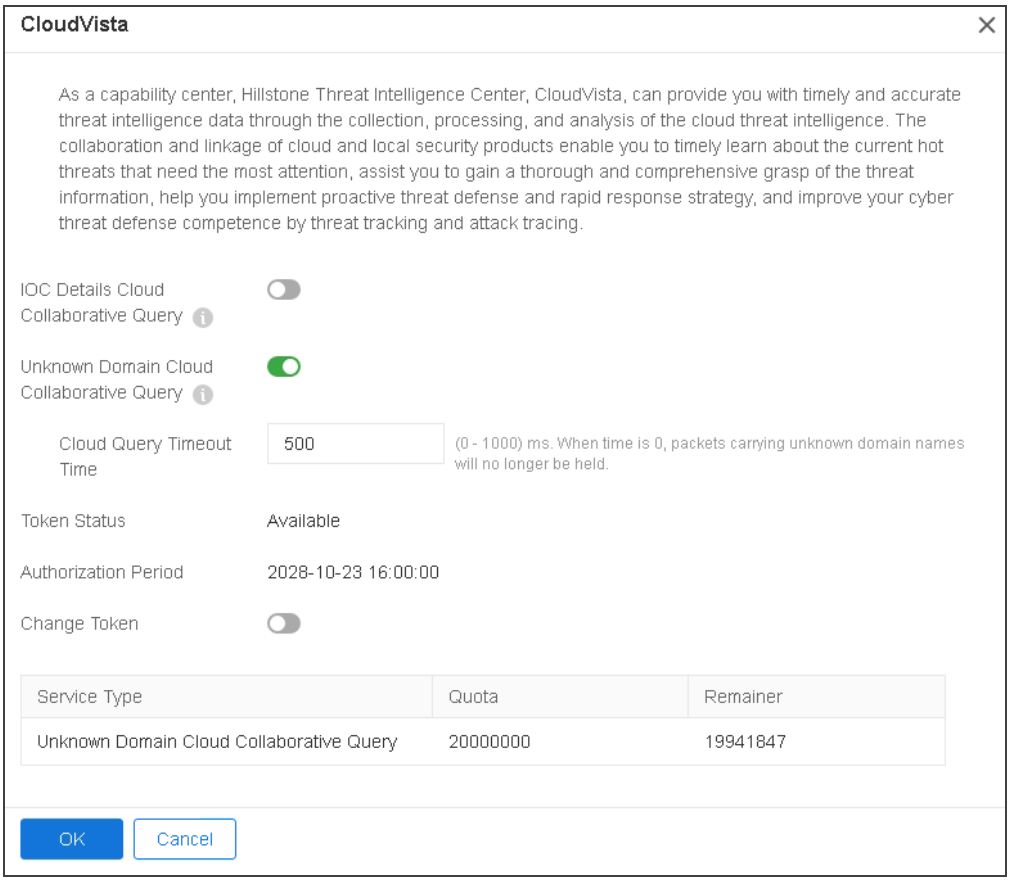
Configuring CloudVista

To define threat detection results via cloud-based data analysis or improve the ability of the Bot-net Prevention function to verify the risk status of unknown domains with the help of cloud-based services, you can use CloudVista.

To configure CloudVista, take the following steps:

1. Select **System > Connecting to Hillstone Cloud Service Platform**.

2. Click **CloudVista**.



3. Configure the **IOC Details Cloud Collaborative Query** function. IOC indicates threat intelligence. This function is used to query detailed threat information from cloud services to assist administrators in analyzing and defining threat detection results. It can be associated with queries in iCenter/Threat Logs.

   Click the button to enable the **IOC Details Cloud Collaborative Query** function. By default, this function is disabled. Once enabled, the function will remain enabled even after a device restart.

> **Notes:** This function is controlled by license. To use it, you need to install Threat Intelligence license first.

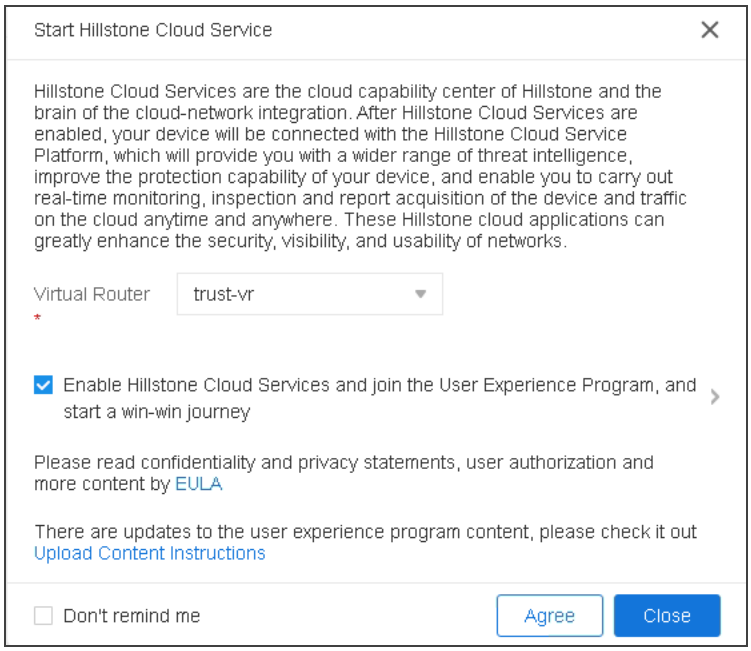
4. Configure the **Unknown Domain Cloud Collaborative Query** function (also known as Cloud Query). This function verifies the risk status of the above unknown domains based on real-time cloud-based query, extending the signature database of the Botnet Prevention function. This enables the Botnet Prevention function to collaborate with Hillstone Threat Intelligence Cloud Service, enhancing DNS traffic analysis, detection, and malicious domain control capabilities.

   For more information about the Token, Cloud Query Timeout Time, Authorization Period, and Service Type/Quota/Remainer parameters, see "Configuring Unknown Domain Cloud Collaborative Query" on Page 1494.

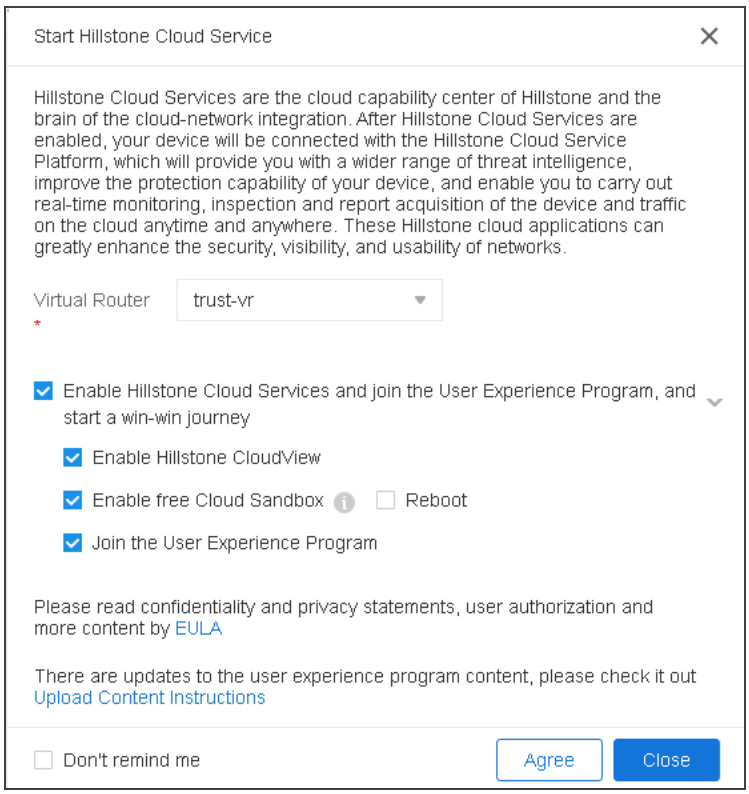
5. Click **OK**.

Enabling Hillstone Cloud Service with One Click

After you log in to the device, the **Start Hillstone Cloud Service** dialog box appears, which recommends that you connect the device to Hillstone cloud platform to obtain more cloud security services.



- Select a virtual router from the **Virtual Router** drop-down list.
- Select **Enable Hillstone Cloud Services and join the User Experience Program, and start a win-win journey** to enable Hillstone CloudView and Cloud Sandbox and join the user experience program. By default, this option is selected. You can also click ◂ to expand the detailed configuration items to enable/disable each service respectively.



Notes: If no Cloud Sandbox license is installed, you can enable free Cloud Sandbox. With this service enabled, the default template "predef_pe" of sandbox will be bound to the specified security zone. You can also manually configure the protection rules and policies of the sandbox. For more information, see Threat Prevention > Sandbox Protection.

- Click **EULA** to view confidentiality and privacy statements, user authorization and more content.
- Click **Upload Content Instructions** to view details about the user experience program.

- Click **Don't remind me** to close the pop-up.
- The notification icon in the upper-right corner displays the number of notifications. You can hover your mouse over the icon to click **UX Update Notification**, and the **Start Hillstone Cloud Service** dialog box appears.

Connecting to iSource

iSource——Intelligent Security Operation System is a holographic data-driven AI analysis and operation system. It is composed of an analysis platform and a wealth of probes. It can provide customers in various industries with functions such as network threat analysis, situation presentation and traceability, and solve customer monitoring blind zones , potential safety hazards, inefficient operation and maintenance and other issues. iSource has the ability to collect holographic data, collect data through various types of data probes, conduct intelligent data mining and analysis based on massive network traffic, threat events and endpoint logs, presenting the global network security and threat situation, and support multiple dimensions core functions such as screencast display, linkage response, and work order make the safe operation of the enterprise under control.

When the device is enabled for connecting to iSource and configured with correct iSource parameters, it can connect to iSource, the iSource can receive and further analyze information about the firewall device. After the firewall device is connected with iSource as a network device, you can upload threat logs and evidence packets to iSource for analysis.



Notes: For more information about iSource, please refer to *iSource User Guide*.

iSource Typical Deployment

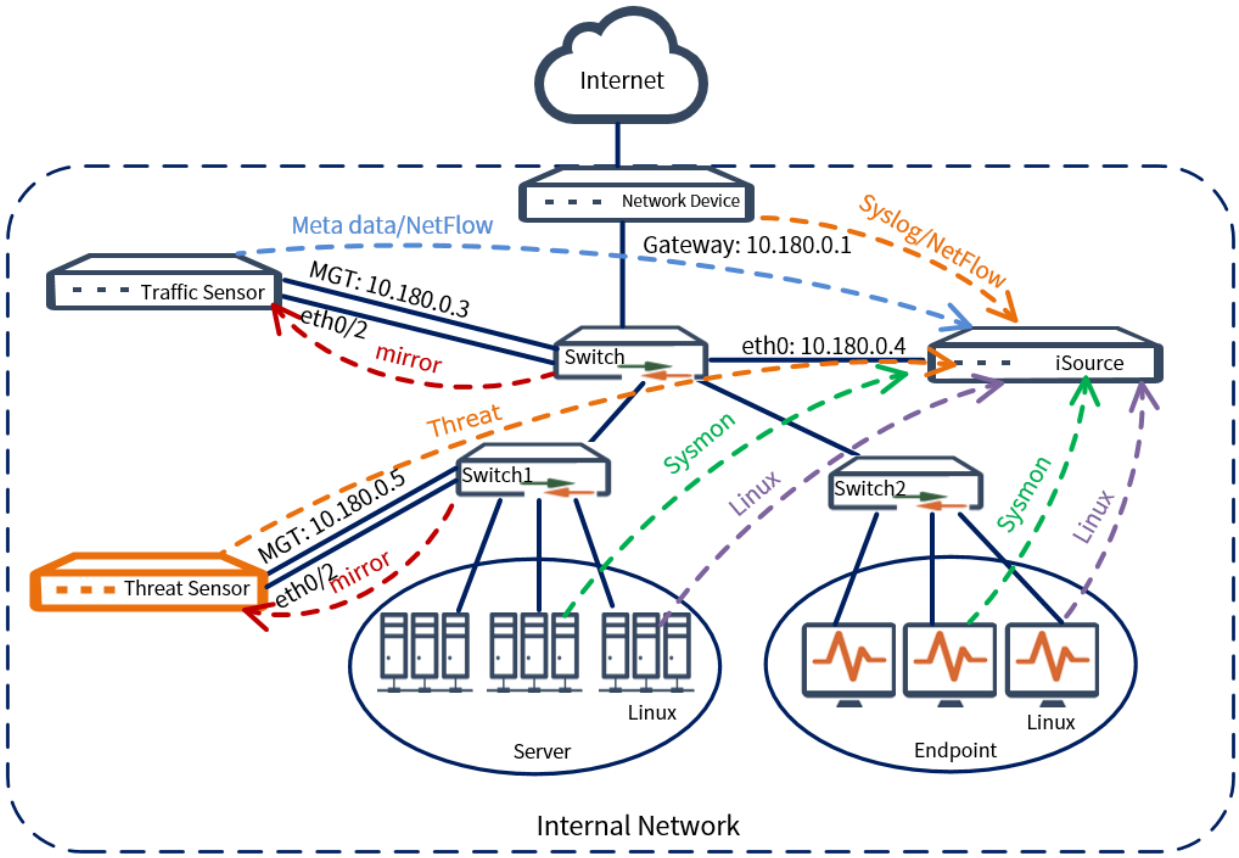
The typical deployment of iSource mainly includes four parts: the iSource Security Operation Platform (referred to as iSource Platform), traffic sensor, threat sensor, and ThreatTrace Client. Typical deployment includes stand-alone deployment and cluster deployment.

Stand-alone Deployment

The iSource platform (single machine) , traffic sensor and threat sensor are deployed in the intranet environment, and the ThreatTrace client is deployed on the user's server or endpoint. After the deployment is completed, the iSource platform can receive information (Meta Data, Syslog, NetFlow, Linux, Sysmon, threat information) from traffic sensor, threat sensor, Linux system

device, network device, and user servers and endpoints, so as to control all network for monitoring and analysis.

The stand-alone deployment scenario is shown in the figure below:



Cluster Deployment

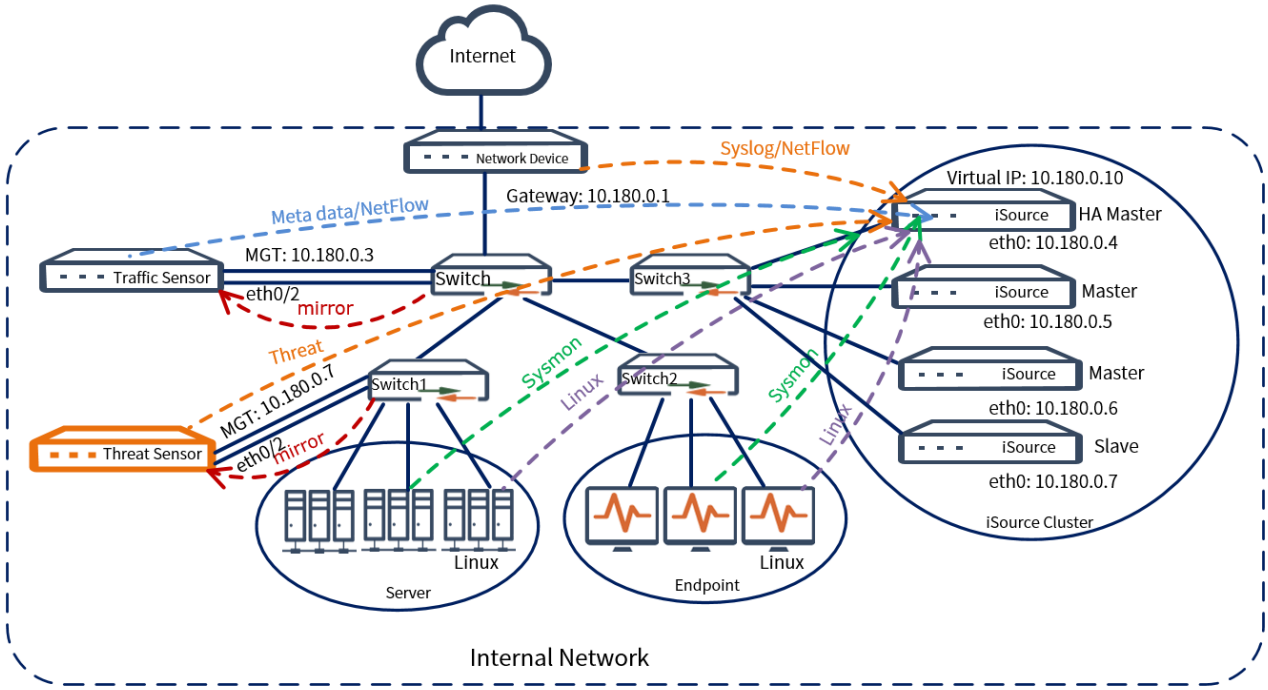
As the amount of user data increases, a single iSource platform may not be able to meet the needs of users. In response to this problem, the iSource platform supports cluster deployment, that is, you can deploy multiple iSource platforms, thereby alleviating the pressure on the data volume of a single iSource platform.

When the number of iSource platforms in the cluster is greater than or equal to 3, the iSource platform cluster will support High Availability (HA) by default, which can provide backup solutions in the event of device failure. When one iSource platform in the cluster fails and becomes unavail-

able, other iSource platforms in the cluster will continue to receive and process data to ensure uninterrupted data communication and effectively enhance the reliability of the network.

Refer to the following cluster deployment topology. The iSource platform (cluster), traffic sensor, and threat sensor are deployed in the intranet environment, and the ThreatTrace client is deployed on the user's server and endpoint. All iSource platforms in the cluster are deployed on the Layer 2 network. The first iSource platform deployed is the HA Master. The HA Master will allocate available resources for other iSource platforms according to its configured internal IP network segment (IP address). After deployment, HA Master can receive all information (Meta Data, Syslog, NetFlow, Linux, Sysmon, threat information) from traffic sensor, threat sensor, Linux system device, network device, and user servers and endpoints, and then transfer the data Information is distributed to other iSource platforms in the cluster through internal IP addresses.

The cluster deployment scenario is shown in the figure below:

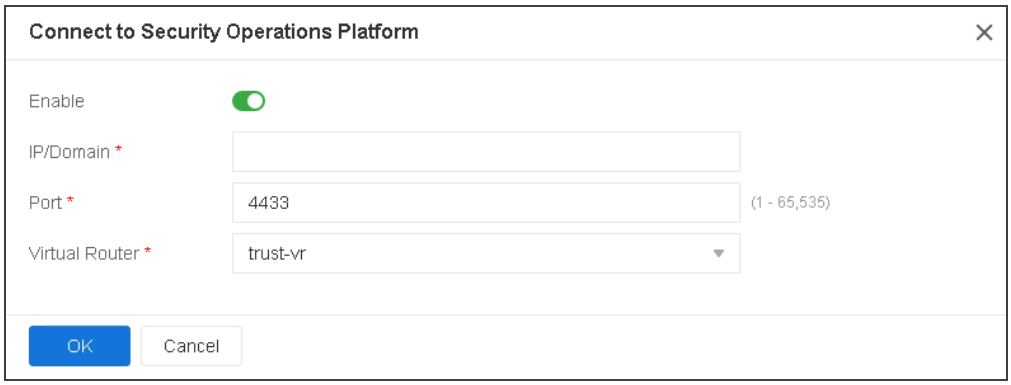


Connecting to iSource

To connect to iSource, take the following steps:

1. Select **System** > **Extended Services**. In the **Connect to Security Operations Platform**, click  in the lower-left corner.

2. Turn on the switch next to Enable.



3. In the IP/Domain field, enter the IP address or domain name.

4. In the Port field, enter the port number that connects to iSource.

5. Select a virtual router from the Virtual Router drop-down list.

6. Click **OK**.

Configuring the Data Types Sent to iSource

To configure the data types sent to iSource after the device is connected to iSource, take the following steps:

1. Select **System** > **Extended Services**. In the **Connect to Security Operations Platform**, click  in the lower-left corner.

2. In the **Data Upload Configuration** section, configure the following options as needed:

   - Turn on the switch next to Threat Log to send threat logs to iSource. By default, this feature is disabled.

- Turn on the switch next to Evidential packets to send threat-related evidential packets captured by the device to iSource. By default, this feature is disabled.
- Turn on the switch next to IoT Asset Monitor to send detected IoT asset data to iSource.

3. Click **OK**.



Notes:

- A-series device, , support to upload threat logs to iSource.
- A-series devices that are installed with SSD , support to upload threat-related evidential packets captured by the device to iSource.

Upgrading System

The firmware upgrade wizard helps you:

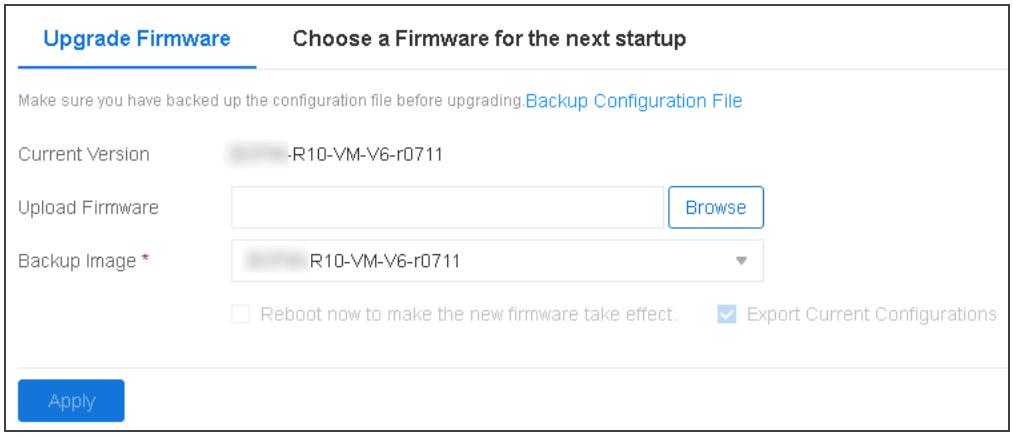
- Upgrade system to a new version or roll back system to a previous version.
- Upgrade the format of earlier-version data such as logs, monitoring data, and reports in the database or delete the data.
- Update the Share Access signature database, Application signature database, URL signature database, Antivirus signature database, Antivirus intelligence file engine database, IPS signature database, Sandbox Whitelist Database, IP reputation database, Risk mitigation rule signature database, Abnormal behavior mode database, Malware behavior mode database, botnet prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database.
- Update the Trusted Root Certificate Database.

Upgrading Firmware

To upgrade firmware, take the following steps:

1. Select **System** > **Upgrade Management** > **Upgrade Firmware**.

2. In the **Upgrade Firmware** tab, configure the following.



Upgrade Firmware	
Backup Configuration File	Make sure you have backed up the configuration file before upgrading. Click **Backup Configuration File** to backup the current firmware file and the system will automatically redirect the Configuration File Management page after the backup.
Current Version	The current firmware version.
Upload Firmware	Click **Browse** to select a firmware file from your local disk.
Backup Image	The backup firmware version.
Export Current Configurations	Select **Export Current Configurations** and click **Apply**. In the tips message, click **OK** to export the current system configuration file to your PC in the .DAT format.
Reboot	Select the **Reboot now to make the new firmware take effect**

Upgrade Firmware	
	check box and click **Apply** to reboot system and make the firmware take effect. If you click **Apply** without selecting the check box, the firmware will take effect after the next startup.
Choose a Firmware for the next startup	
Select the firmware that will take effect for the next startup.	Select the firmware that will take effect for the next startup.
Export Current Configurations	Select **Export Current Configurations** and click **Apply**. In the tips message, click **OK** to export the current system configuration to your PC in the .DAT format.
Reboot	Select the **Reboot now to make the new firmware take effect** check box and click **Apply** to reboot system and make the firmware take effect. If you click **Apply** without selecting the check box, the firmware will take effect after the next startup.

Notes: StoneOS 5.5R10P3 and later support to remotely upgrade the system version of the device by using CloudView.

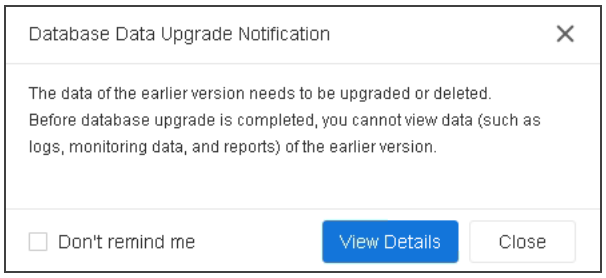
Upgrading Database Data

After you upgrade the system to a new version, both the earlier and new versions of data, such as logs, monitoring data, and reports, exist in the database. Due to the format inconsistency between these two versions of data, you may not be able to view the earlier version of data. To ensure that system features can be displayed and used properly, you need to upgrade the earlier version of

data in the database to the data in the format that complies with the new version. If you do not need the earlier version of data, delete it.

Notes: Only manual database data upgrade is supported.

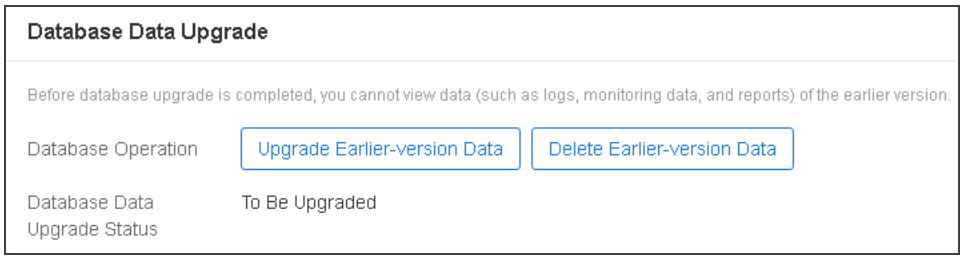
If earlier version of data exists in the system, a message that reminds you to upgrade data appears when you log into the system. You can view the data before the upgrade is completed.



- Select **Don't remind me** to close the dialog box. To view the dialog box again, hover your mouse over the notification icon in the upper-right corner and select **Database Data Upgrade Notification** from the drop-down list.
- Click **View Details** to upgrade or delete database data on the Database Data Upgrade page.

To upgrade database data, take the following steps:

1. Select **System** > **Upgrade Management** > **Database Data Upgrade**.
2. Configure the following options:



Option	Description
Database Oper-	You can upgrade or delete earlier-version data in the system

Option	Description
ation	database. • Upgrade Earlier-version Data: If you click this option, you can upgrade earlier version of data whose format is inconsistent with that of new version of data. • Delete Earlier-version Data: If you click this option, you can delete earlier version of data whose format is inconsistent with that of new version of data. This operation does not affect other data whose format complies with the format of the new version of data. Note: If the system is downgraded to a lower version, **To Be Upgraded** is displayed in the Database Data Upgrade Status field. In this case, you can click **Upgrade Earlier-version Data** to downgrade database data to data in the format that complies with the new version. For more information about how to downgrade the system version, see Upgrading Firmware.
Database Data Upgrade Status	Displays the upgrade status of data in the system database. • To Be Upgrade: If earlier version of data whose format is inconsistent with that of new version of data exists in the system, this status is displayed. • Upgrading: If earlier version of data whose format is inconsistent with that of new version of data exists in the system, this status is displayed after you click **Upgrade Earlier-version Data**. In the meantime, the upgrade progress and the time consumed are displayed. • Upgrade Not Required: If earlier version of data is upgraded or deleted, this status is displayed because all

Option	Description
	database data are in the complied format.

Updating Signature Database

The signature databases that can be installed include Encrypted traffic detection database,Share Access signature database,Application signature database, URL signature database, Antivirus signature database, antivirus intelligence file engine database, Sandbox Whitelist Database, IPS signature database, IP reputation database, SSL proxy domain whitelist signature database, Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database. Except Encrypted traffic detection database,SSL proxy domain whitelist signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database, you can only view other signature databases when the system is installed with the corresponding licenses. The system support the following two methods to upgrade signature databases: remote update via HTTP and HTTPS; local update via downloading update package through the default signature database update server.Except the SSL proxy domain whitelist signature database or ISP Information Database, you can only view signature databases installed with licenses.

The system supports to download each signature database over IPv6.

Notes:

The following devices support to antivirus intelligence file engine database.

- A-series: Except SG-6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800, and SG-6000-A2200.

To update signature database, take the following steps:

1. Select **System** > **Upgrade Management** > **Signature Database Update**.

2. In the **Signature Database Update** page, configure the following.

Option	Description
Current Version	Show the current version number.
Latest Version	Show the latest version number. **Note:** The latest version of the ISP information database can be displayed only when the current version exists. The latest version of other signature databases can be displayed only when the corresponding signature database licenses are activated and the current version exists.
Remote Update	Encrypted traffic detection database, Application signature database, URL signature database, Antivirus signature database, IPS signature database , IP reputation database , Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geography database. • Protocol: Select the update method of the signature database, including HTTP and HTTPS. Click **Restore Default** to restore the default HTTPS transmission method. • Update Server: By default the system updates the signature database everyday automatically. You can change the update configuration as needed. The IPv4 and IPv6 address are supported for configuring the update server address. Hillstone devices provide two default update servers: https://update1.hillstonenet.com and https://up-

Option	Description
	date2.hillstonenet.com. You can customize the servers according to your need. In **Update Server**, specify the server IP or domain name and Virtual Router. • Update Proxy Server: When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature database can update normally. In **Update Proxy Server**, enter the IP addresses and ports of the main proxy server and the backup proxy server. • Auto Update: Click the **Enable** button of **Auto Update** and specify the auto update time. Click **Ok** to save your changes. • Update Now: Click **Ok And Online Update** to update the signature database right now.
Local Update	Download the update package from the default feature update server for local update. • Download the upgrade packages of the encrypted traffic detection database, application signature database, URL signature database, Antivirus signature database, IPS signature database , IP reputation database, SSL proxy domain whitelist signature database, , Botnet Prevention signature database, MITRE ATT&CK® knowledge base, ISP information database, and IP geo-

Option	Description
	graphy database from https://update1.hillstonenet.com and https://update2.hillstonenet.com. • Click **Browse** and select the signature file in your local PC, and then click **Upload**. **Notes:** 1. Before StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Botnet C&C Detection Package" link of the default update server. From StoneOS R8P4 version, please download the Botnet Prevention signature database upgrade package through the "Encrypt Botnet C&C Detection Package" link of the default update server. 2. If a large number of devices (with the same version and model) need local update, contact Hillstone's support team to acquire bulk update solutions.

Updating Trusted Root Certificate Database

To ensure that the root certificates stored on your device are sufficient and up-to-date, and to reduce errors occurred during server certificate verification, you need to update the trusted root certificate database timely. System supports both remote upgrade and local upgrade. When updating the trusted root certificate database, system will delete revoked certificates and expired certificates, and add new certificates.

To update the trusted root certificate database, take the following steps:

1. Select **System** > **Upgrade Management** > **Trusted Root Certificate Update**.

2. In the **Trusted Root Certificate Update** page, configure the following.

Option	Description
Current Version	Show the current version number.
Remote Update	Click **Remote Update** and configure the following update parameters. • Update Server: By default, system updates the trusted root certificate database everyday automatically. You can change the update configuration as needed. Hillstone devices provide two default update servers: https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can customize the servers as needed. Under **Update Server**, specify the server IP or domain name and virtual router. • Update Proxy Server: When the device accesses the Internet through an HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server to ensure the trusted root certificate database can be updated normally. Under **Update Proxy Server**, enter the IP addresses and ports of the main proxy server and the backup proxy server. • Auto Update: Click the **Enable** button and specify the auto update time. Click **OK** to save your changes.

Option	Description
	• OK And Online Update: Click the button to update the trusted root certificate database immediately.
Local Update	Click **Local Update**, and click **Browse** to select a trusted root certificate database file in your local PC, and then click Upload.

License

Licenses are used to authorize the users' features, authorize the users' services, or extend the performance. If you do not buy and install the corresponding license, the features, services, and performance which is based on the license will not be used or cannot be achieved.

Platform License	Description	Valid Time	Whether to Restart
Platform Trial	Platform license is the basis of the other licenses operation. If the platform license is invalid, the other licenses are not effective. The device have been pre-installed platform trial license for 15 days in the factory.	You cannot modify the existing configuration when License expires. If the device is restarted, the previous configuration is retained but cannot be modified.	Not required.
Platform	You can install the platform license after the device formal sale. The license	System cannot upgrade the OS version when the	Not required.

	provide basic firewall and VPN function.	license expires, but the system could still work normally.	
Function License	**Description**	**Valid Time**	**Whether to Restart**
VSYS	Authorizing the available number of VSYS.	Permanent	Restart is required for each installation.
SSL VPN Trial License	Authorizes the maximum number of SSL VPN users that can be connected to the platform. The duration of use of the license is short. The actual available duration is determined by the protocol for the license. The available duration is a relative time, such as 30 days. Multiple SSL VPN trial licenses can be used together.	After the trial license expires, the number of SSL VPN users that can be connected to the platform is restored to its prior value.	No
SSL VPN	Authorizing the number of SSL VPN access. Through installing multiple SSL VPN	Permanent	All versions, except the fol-

	licenses, you can add the number of SSL VPN access.		lowing should be restarted after each installation. Versions that do not need restarting are5.5R6P21 and later 5.5R6P versions, 5.5R8P7 and later 5.5R8P versions, 5.5R9 and later.
ZTNA	Authorizing the maximum number of ZTNA access. ZTNA license has a higher priority than the ZTNA trial license. Multiple ZTNA licenses can be installed to increase the authorized number of ZTNA access. When the authorized number of SSL VPN access is inadequate, SSL VPN access can	Permanent	ZTNA

	use the ZTNA license. ZTNA access cannot use the SSL VPN license.		
ZTNA Upgrade	Converting the specified number of SSL VPN access to the equal number of ZTNA access. The SSL VPN license type is not limited. Multiple ZTNA Upgrade Licenses can be installed, but the converted number of access cannot exceed the total number of SSL VPN access. If the converted SSL VPN license is not permanent, the validity period of the ZTNA license is the same as the SSL VPN license before the conversion.	Permanent	ZTNA Upgrade
ZTNA Trial	Providing ZTNA trial. Multiple ZTNA trial licenses can be installed to increase the number and validity period of ZTNA access.	When the license expires, you can only use the default authorization of 8 ZTNA con-	ZTNA Trial

		current users.	
QoS	Enable QoS function.	Permanent	Not required.
Cloud sandbox License	Providing Cloud sandbox function and white list update, authorizing the number of suspicious files uploaded per day. Including 4 licenses: Cloud sandbox-200, Cloud sandbox-300, Cloud sandbox-500 and Cloud sandbox-1000. The number of files allowed to upload per day is different for different licenses.	The valid time including 1 year, 2 years and 3 years. System cannot analyze the collected data and cannot update the white list when the license expires. The Cloud sandbox protection function can only be used according to the local database cache results. If you restart the device, the function cannot be used.	Restart is required for the first installation. Do not require restart when you renew the subscription.
Twin-mode License	Providing the twin-mode function. The related parameters of the twin-mode function can be displayed	System cannot upgrade the twin-mode function and cannot	Not required.

	and configured.	provide the maintenance service when License expired.	
EPP	Providing the End Point Prevention function.	The End Point Prevention function cannot be used when the license expires.	Not required.
Service License	**Description**	**Valid Time**	**Whether to Restart**
AntiVirus	Providing antivirus function, and antivirus signature database and antivirus intelligence file engine database update. Note:Devices except SG-6000-A200, SG-6000-A200W, SG-6000-A200G4B, SG-6000-A1600, SG-6000-A1800 and SG-6000-A2200 support the antivirus intelligence file engine database.	System cannot update the anti-viru signature database when the license expires, but the antivirus function could still be used normally	Restart is required for the first installation. Do not require restart when you renew the subscription.
AntiVirus Trial License	Providing trial use of anti-	After the trial	Restart is

	virus function, and antivirus signature database and anti-virus intelligence file engine databaseupdate. After you install the anti-virus trial license, the system supports the same antivirus function as the antivirus license. The duration of use of the trial license is short. You can select an available duration when applying the license, which cannot exceed 90 days. Multiple antivirus trial licenses can be used together.	license is expired, you can no longer use the antivirus function and intel-ligence file engine-detection function, and you cannot upgrade the antivirus sig-nature database and antivirus intel-ligence file engine database.	required for the first install-ation. Do not require restart when you add more trial licenses. After the license is expired, restart is required for installing a new license.
URL DB	Providing URL database and URL signature database update.	System cannot provide the search URL data-base online func-tion when the license expires, but the user-defined URL and URL filtering function can be used normally.	Restart is required for the first install-ation. Do not require restart when you renew the sub-scription.

IPS	Providing IPS function and IPS signature database update.	System cannot update the IPS signature database when the license expires, but the IPS function could still be used normally.	Restart is required for the first installation. Do not require restart when you renew the subscription.
IPS Trial License	Providing IPS function and IPS signature database update. After you install the IPS trial license, the system supports the same IPS function as the IPS license. The duration of use of the trial license is short. You can select an available duration when applying the license, which cannot exceed 90 days. Multiple IPS trial licenses can be used together.	After the license is expired, you can no longer use the IPS function and upgrade the IPS signature database.	Restart is required for the first installation. Do not require restart when you add more trial licenses. After the license is expired, restart is required for installing a new license.
APP signature	APP signature license is issued with platform license, you do not need to apply alone. The valid time of	System cannot update the APP signature database when the license	Not required.

	license is same as platform license.	expires, but the included functions and rules could still be used normally.	
Threat Prevention	A package of features, including AntiVirus, IPS, threat intelligence, and corresponding signature database update.	System cannot update all signature databases when the license expires, but the included functions and rules could still be used normally.	Whether to restart, please refer to the restart policies for the individual licenses of AntiVirus, IPS, threat intelligence.
IP Reputation	Providing Perimeter Traffic Filtering function of IP reputation and IP reputation database update. From 5.5R6, StoneOS will support the Perimeter Traffic Filtering function of IP Reputation instead of predefined black list. You can buy the license of IP reputation to upgrade.	System cannot update the IP reputation database when the license expires.	Restart is required for the first installation. Do not require restart when you renew the subscription.
Antispam	Providing Anti-Spam function.	The Anti-Spam function cannot	Restart is required for

		be used when the license expires.	the first installation. Do not require restart when you renew the subscription.
Botnet Prevention	Providing Botnet Prevention function and Botnet Prevention database update.	System cannot update all signature databases when license expires. But the functions included and rules could be used normally.	Restart is required for the first installation. Do not require restart when you renew the subscription.
Botnet Prevention Trial License	Providing the trial use of botnet prevention function and botnet prevention signature database update. After you install the botnet prevention trial license, the system supports the same botnet prevention function as the antivirus license. The duration of use of the trial license is short. You can	After the license is expired, you can no longer use the botnet prevention function and upgrade the botnet prevention signature database.	Restart is required for the first installation. Do not require restart when you add more trial licenses. After the license is expired, restart is required for

	select an available duration when applying the license, which cannot exceed 90 days. Multiple botnet prevention trial licenses can be used together.		installing a new license.
IoT monitor&control	Providing the IoT policy function.	Permanent.	Not required.
IoT monitor&control trail	After the installation of IoT monitor&control trail license, you will get the same IoT policy function as system with IoT monitor&control license. But the duration will be shorter.	The IoT policy function cannot be used when the license expires. If you restart the device, the existing IoT policy configurations will not be lost, but won't take effect.	Not required.
IoT video monitoring	Providing IoT Policy function and authorizing the maximum number of IoT devices that can be identified and then monitored. • If multiple IoT video monitoring licenses	Permanent	

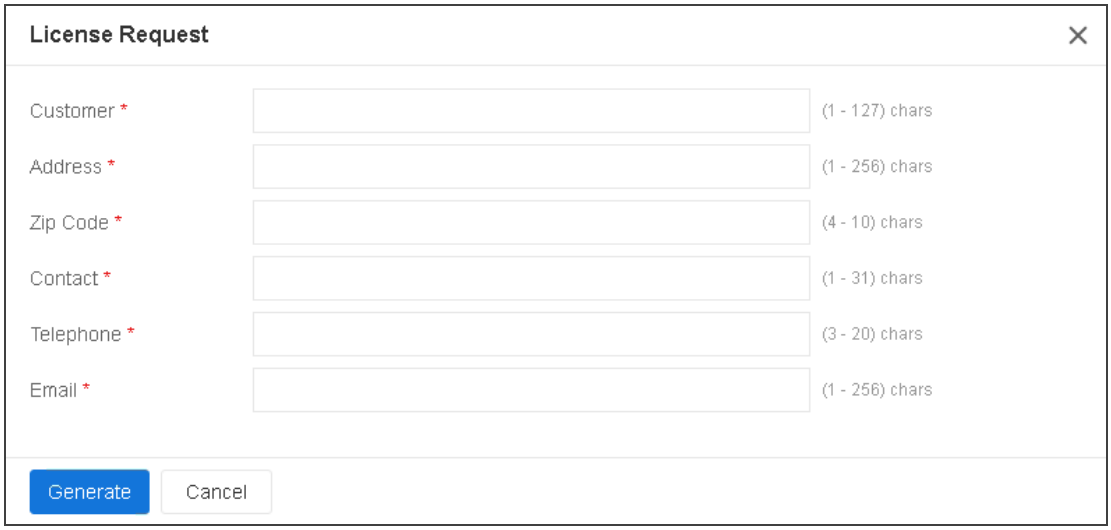
	are installed on the system, the maximum number of monitored IoT devices can be accumulated. • If both IoT monitor&control license and IoT video monitoring license are installed on the system, the maximum number of monitored IoT devices is determined by the IoT monitor&control license. • The existing IoT monitor&control license becomes invalid upon the installation of the IoT video monitoring license.		
Threat intelligence License	Providing the threat intelligence function.	The threat intelligence function cannot be used when the license expires.	Not required.

Bundle License1	A package of features, including IPS, AntiVirus, threat intelligence, QoS, URL DB, and corresponding signature database update.	For expiration, refer to the respective license policy.	Whether to restart, please refer to the restart policies for the individual licenses of IPS, AntiVirus, threat intelligence, QoS, URL DB.
Bundle License3	A package of features, including IPS, AntiVirus, threat intelligence, QoS, URL DB, Botnet Prevention, IP Reputation, Cloud sandbox, and corresponding signature database update.	For expiration, refer to the respective license policy.	Whether to restart, please refer to the restart policies for the individual licenses of IPS, AntiVirus, threat intelligence, QoS, URL DB, Botnet Prevention, IP Reputation, Cloud sandbox.

Applying for a License

Before you apply for a license, you have to generate a license request first.

1. Click **Apply For**. Under License Request, input user information. All fields are required.



2. Click **Generate**, and then appears a bunch of code.

3. Send the code to your sales contact. The sales person will issue the license and send the code back to you.

Installing a License

After obtaining the license, you must install it to the device.

To install a license, take the following steps:

1. Select **System** > **License** , and click **Import**.

2. On the **Import License** page, configure options below.

Option	Description
Upload License File	Select **Upload License File**. Click **Browse** to select the license file, using the TXT format, and then click **OK** to upload it.

Option	Description
Manual Input	Select **Manual Input**. Type the license string into the box.

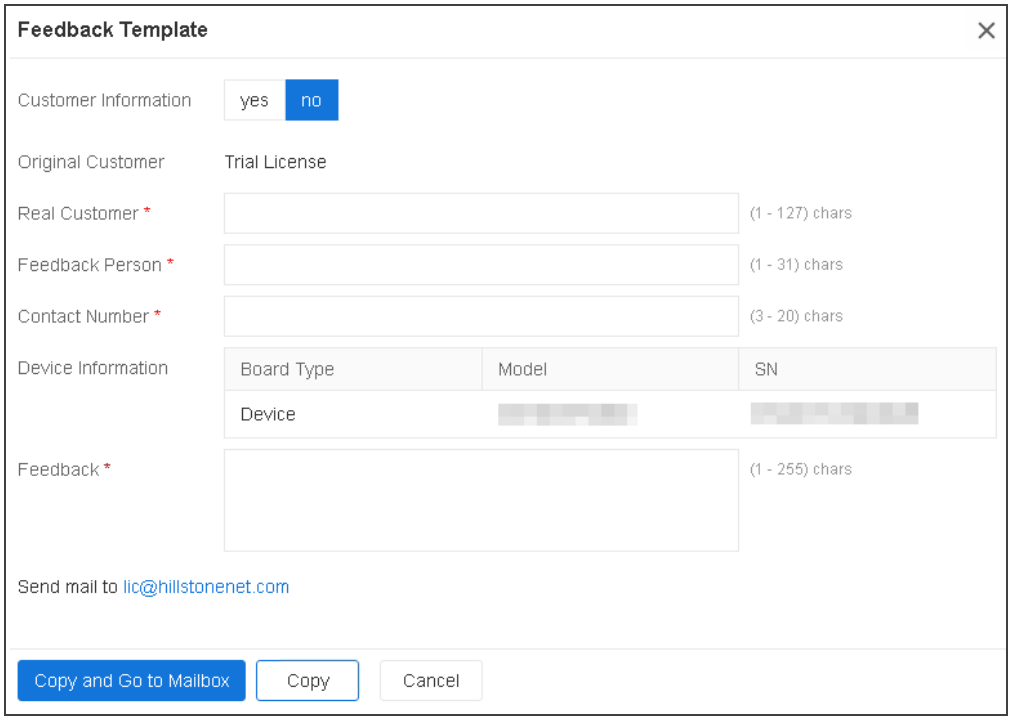
3. Click **OK**.

Feedback Template

The system supports the feedback template. When you use the device, if you find that the information in the license is different from the actual information or encounter other issues related to license, you can use the template to enter a feedback, and then copy and send the feedback to the email address lic@hillstonenet.com. If you do not provide a feedback, the service validity may be affected.

To provide a feedback, take the following steps:

1. Select **System** > **License**, and enter the License List page.
2. Click **Feedback Template** in the prompt at the top of the page.



On the Feedback Template page, configure options below.

Option	Description
Customer Information	Check if the customer name corresponding to the current platform license is correct on the License List page. • When **Yes** is selected, the current customer name is displayed in the Customer , which cannot be edited. • When **No** is selected, the current customer name is displayed in the **Original Customer**, which cannot be edited. You can fill in the correct customer name in the text box at the **Real Customer** with a range of 1 to 127 characters.
Feedback Person	Fill in the name of the feedback person, ranging from 1 to 31 characters.
Contact Number	Fill in the contact number of the feedback person, ranging from 3 to 20 characters.
Device Information	Display the device information of the current device. • Devices except X-Series: Display the corresponding model and SN of the device. • X-series devices: Display the corresponding model and SN of the frame, as well as the model and SN of the expansion module installed in the expansion slot.
Feedback	Describe the issues that require feedback, ranging from 1 to 255 characters.

3. Click **Copy and Go to Mailbox** to jump to the mailbox and paste the above content into the mail; Or click **Copy** to copy the above content and manually paste it into the mail.

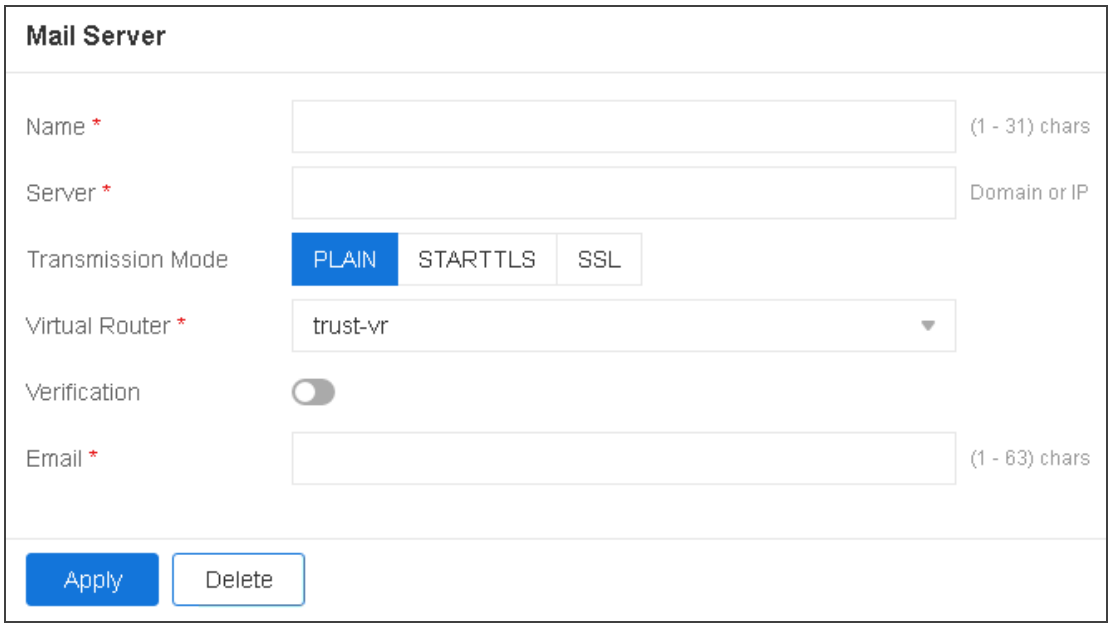
Mail Server

By configuring the mail server in the Mail Server page, the system can send the log messages, report or alarm information to the specified email address.

Creating a Mail Server

To create a mail server, take the following steps:

1. Select **System** > **Mail Server**.



2. In the Mail Server Configuration page, configure these values.

Option	Description
Name	Type a name for the mail server into the box.
Server	Type Domain name or IP address for the mail server into the box.
Transmission Mode	Select the transmission mode for the email. • PLAIN: Specifies that the mail is sent in plain text and is not encrypted. This mode is the default transmission mode. • STARTTLS: STARTTLS is an extension to the plain text communication protocol that upgrades plain text connections to encrypted connections. Specified in this mode, the mail will be transmitted using encrypted mode. • SSL: SSL protocol is a security protocol that provides security and data integrity for network communication. Specified in this mode, the mail will be transmitted using encrypted mode.
Port	Type the port number for the mail server into the box. The range is 1 to 65535. The default port number is different for different transmission modes, PLAIN: 25, STARTTLS: 25, SSL: 465.
Virtual Router	From the **Virtual Router** drop-down list, select the Virtual Router for the SMTP server.

Option	Description
Verification	Select the **Enable** check box for mail verification to enable it if needed. Type the username and its password into the corresponding boxes.
Email	Type the email address that sends mail.

3. Click **Apply**.

SMS Parameters

This Section contains the following contents:

- "SMS Modem" on Page 1814
- "SMS Gateway" on Page 1815

SMS Modem

An external GSM modem device is required for sending SMS messages. First, you need to prepare a mobile phone SIM card and a GSM SMS Modem . Insert the SIM card into your modem and then, connect the modem and the firewall using a USB cable.

The following one models of SMS modem is recommended:

Model	Type	Interface
4G MODEM M1806-NC5	LTE(FDD) LTE(TDD) WCDMA TD-SCOMA GSM/GPRS/EDGE CDMA2000	USB interface
GSM MODEM M1206B	GSM	USB interface

System will show the modem connection status: correctly connected, not exist or no signal.

Configuring SMS Parameters

You can define the maximum SMS message number in one hour or in one day. If the messages exceed the maximum number, system will not make the modem to send messages, but it will keep a log for this behavior.

Option	Description
Maximum messages per hour	Defines the maximum message number the modem can send in one hour.
Maximum messages per day	Defines the maximum messages number the modem can send in one day.

Testing SMS

To test if the message sending works, you can send a test text to a mobile.

To send a text message to a specified mobile number, take the following steps:

1. Select **System > SMS Parameters**.
2. Enter a mobile phone number in the text box.
3. Click **Send**. If the SMS modem is correctly configured and connected, the phone using that number will receive a text message; if it fails, an error message will indicate where the error is.

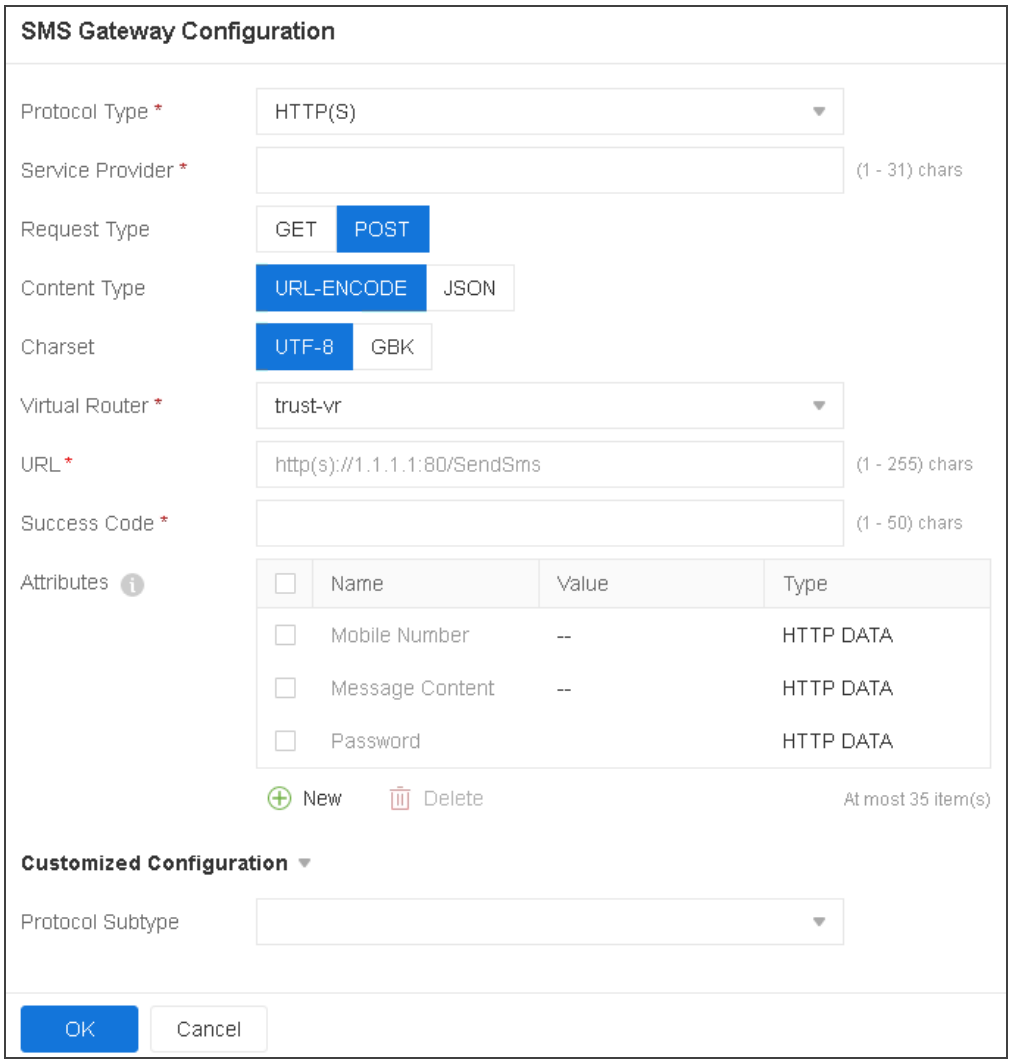
SMS Gateway

Configuring SMS Gateway

To configure the SMS gateway, take the following steps:

1. Select **System > SMS Parameters >SMS Gateway**.

2. Click **New**.



Option	Description
Protocol Type	Specifies the protocol of SMS gateway. SGIP indicates the SGIP protocol of Chinaunicom. UMS indicates the enterprise information platform of Chinaunicom. ACC indicates the ACC protocol of Chinatelecom. ALIYUNSMS indicates the SMS service platform of Alibaba Cloud. XUANWU

Option	Description
	indicates the Xuanwu Technology SMS service platform. CAS indicates the 12302 SMS service platform. BEIKE indicates BEIKE SMS gateway. ChinaMobileMusic indicates the SMS platform of China Mobile Music. HTTP(S) indicates HTTP/HTTPS protocol.
Service Provider	Specifies the service provider name. The value range is 1 to 31.
Request Method	When the HTTP (S) protocol type is specified for the SP instance, you can specify the request method of HTTP(S). The default request method is POST.
Content Type	When the HTTP (S) protocol type is specified for the SP instance, you can specify the content type of HTTP Post requests sent to the SMS gateway. By default, URL-ENCODE is selected. • URL-ENCODE - Sets the content type of HTTP POST requests to application/x-www-from-urlencode. • JSON - Sets the content type of HTTP POST requests to application/json.
Charset	When the HTTP (S) protocol type is specified for the SP instance, you can specify the charset of HTTP(S). The default charset is UTF-8.
UMS Protocol	When the protocol type is specified as "UMS", users can spe-

Option	Description
	cify the UMS protocol type. The default protocol type is HTTPS.
Protocol	When the protocol type is specified as "ACC", "ALIYUNSMS", "CAS" or BEIKE, users can specify the protocol type. When the protocol type is specified as "CAS", the default protocol type is HTTPS. The default protocol type is HTTP for ACC and ALIYUNSMS, and HTTPS for BEIKE.
Virtual Router	Specifies the VRouter which gateway belongs to. The system supports multi-VR, and the default VR is trust-vr.
URL	When the HTTP (S) or the ChinaMobileMusic protocol type is specified for the SP instance, you can specify the URL of HTTP(S). You need to enter a complete access path, such as "http(s)://1.1.1.1:80/SendSms". The system requests to communicate with the SMS gateway based on the specified URL address. The range is 1 to 255 characters.
Source Mobile Number	When the ChinaMobileMusic protocol type is specified for the SP instance, you can specify the mobile number used to send verification code messages. The value can be an 8-digit to 21-digit number.
Platform ID	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the ID of China Mobile Music SMS Platform, which is provided by China Mobile

Option	Description
	Music SMS Platform. The ID is a 4-digit number.
Platform Password	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the password used to log in to China Mobile Music SMS Platform. The password is provided by China Mobile Music SMS Platform. The password is 1 to 64 characters.
Confirm Password	Re-type the password into the **Confirm Password** box.
Platform Subsystem ID	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the subsystem ID of China Mobile Music SMS Platform, which is provided by China Mobile Music SMS Platform. The ID is a 3-digit number or 7-digit number.
Template ID	When the ChinaMobileMusic protocol type is specified for the SP instance, you can configure the template ID of verification code messages, which is provided by China Mobile Music SMS Platform. The ID is a 1-digit to 21-digit number.
Success code	When the HTTP (S) protocol type is specified for the SP instance, you can specify the success code of HTTP(S). Success code is used to determine whether the SMS gateway successfully sent an authentication message. Refer to the status code in the SMS gateway manual. For example, if an SMS gateway sent an authentication message successfully, the status code returned is "OK: 325689", and if failed, the

Option	Description
	status number returned is "ERROR: eUser". In this instance, you can specify the success code as "OK". The range is 1 to 50 characters.
Attributes	When the HTTP (S) protocol type is specified for the SP instance, you can configure attributes to communicate with the SMS gateway. • The mobile number field specifies the parameter name of the mobile number. This is a default attribute and must be specified. The range is 1 to 20 characters. You can also configure Node Name and Array Object for the field. • The message content field specifies the parameter name of the authentication message. This is a default attribute and must be specified. The range is 1 to 20 characters. You can also configure Node Name and Array Object for the field. • The password field specifies the parameters of password to log in the SMS gateway. The parameter name and parameter value must exist at the same time or be empty. This is an optional attribute. The range of parameter name is 1 to 20 characters and the range of parameter value is 1 to 255 characters. You can also configure Node Name and Array Object for the field. • Click **New** and configure the parameter name, parameter value, parameter type, node name, and array object of the custom attribute of the user to log in to

Option	Description
	the SMS gateway. • Name: The range is 1 to 20 characters. • Value: The range is 1 to 255 characters. • Type: You can set the type to HTTP DATA or HTTP HEADER. If the type is set to HTTP DATA, the attribute will be used as data content of HTTP. If the type is set to HTTP HEADER, the attribute will be added to the header of HTTP. • Node Name: Enter the node name, which can contain only letters, numbers, and underscores. The range is 1 to 20 characters. After you specify the node name, the system constructs packets when sending text messages by combining the attributes belonging to the same node name in the HTTP message in the JSON format. You can configure 10 different node names. • Array Object: Sets the attribute to array object. This way, the parameter values are stored in array. To do this, click ×. When ✓ is displayed, it indicates that the attribute is set to array object. You can create new attributes as needed, with up to 32 at the same time. Select the check box of the attributes bar

Option	Description
	and click "Delete". Note: • Node name and array object can be configured only when the method is POST, content type is JSON, and parameter type is HTTP DATA. • For the attribute fields with the same node name, the array object configurations need to be consistent. • The parameter name of the mobile number field, message content field, and password field can be the same. For other attributes, the parameter name can be the same only if the parameter types are different.
Protocol Subtype	If the protocol type is set to HTTP(s), you can select MAS, EMAY, or ZGC from the drop-down list to connect the Hillstone device to the mobile cloud MAS SMS platform, EMAY SMS, or ZGC SMS platform. To specify the MAS protocol subtype, you need to configure the following attributes in the Attributes section above: • mobiles: Sets the name of the mobile number field to mobiles. This attribute is required. • content: Sets the name of the SMS content field to content. This attribute is required. • secretKey: Specifies the name and value of the pass-

Option	Description
	word used to log in to the SMS gateway. The name needs to be "secretKey" and the value can be 1 to 255 characters in length. This attribute is required. • apId: Click **New** and specify the name, value, and type of the username used to log in to the SMS gateway. The name needs to be "apId", the value can be 1 to 255 characters in length, and the type needs to be "HTTP DATA". This attribute is required. • ecName: Click **New** and specify the name, value, and type of the enterprise name field. The name needs to be "ecName", the value can be 1 to 255 characters in length, and the type needs to be "HTTP DATA". This attribute is required. • sign: Click **New** and specify the name, value, and type of the signature code field. The name needs to be "sign", the value is provided by China Mobile Cloud MAS SMS Platform, and the type needs to be "HTTP DATA". This attribute is required. • addSerial: Click **New** and specify the name, value, and type of the extension code field. The name needs to be "addSerial", the value is provided by China Mobile Cloud MAS SMS Platform, and the type needs to be "HTTP DATA". This attribute is optional. **Note:**

Option	Description
	• When you specify the MAS protocol subtype, to connect the Hillstone device to the mobile cloud MAS SMS platform, the request type needs to be "POST"; the content type needs to be "JSON"; and the charset needs to be "UTF-8". • When you specify the EMAY protocol subtype, to connect the Hillstone device to the EMAY SMS platform, the request type needs to be "POST" and the content type needs to be "JSON".
Host	Specifies the gateway address.
Port	Specifies the port number of the gateway. When the protocol type is specified as "SGIP", the default port number is 8801; When the protocol type is specified as "ACC", the default port number is 80; When the protocol type is specified as "BEIKE", the default port number is 8086; When the protocol type is specified as "UMS", the default port number is 9600. When the protocol type is specified as "XUANWU" or "CAS", the default port number is 8080.
Device Code	Specifies the device code, the range is 1 to 4294967295. When the protocol type is specified as "SGIP", and before configuring the SMS gateway, you have to ask your supplier to provide the device ID of SP, which sends the SMS messges.
Source Number	When the protocol type is specified as "SGIP", and aftering enabling the SMS Authentication function, the system will

Option	Description
	send an Auth-message to the mobile phone number. Specifies the user's phone number, the range is 1 to 21.
Company Code	When the protocol type is specified as "UMS", users can specify the enterprise code registered on the UMS platform. The range is 1 to 31 digits.
Username	Specifies the username to log in SMS gateway. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1-31. When the protocol type is specified as "XUANWU", the range is 1-6.
Password	Specifies the password for the user. When the protocol type is specified as "UMS", "SGIP" or "CAS", the range is 1-31. When the protocol type is specified as "XUANWU", the range is 1-6.
Template Name	Specifies the template parameter of BEIKE SMS gateway.
Confirm Password	Re-type the password into the **Confirm Password** box to confirm.
Change Password	When you edit the SMS gateway, you can see the Change Password function. After you enable this function, the Password field is displayed. To change the password, enter a new one in this field and save the configuration.
SMS Limit/hour	Defines the maximum message number the gateway can send in one hour.
SMS Limit/day	Defines the maximum messages number the gateway can

Option	Description
	send in one day.
AccessKeyId	Specifies the AccessKeyId which will be used as the user-name for authentication between the device and the SMS gateway of Alibaba Cloud. This parameter should be the same with the template AccessKeyId applied in the SMS of Alibaba Cloud.
AccessKeySecret	Specifies the AccessKeySecret which will be used as the password for authentication between the device and the SMS gateway of Alibaba Cloud. This parameter should be the same with the template AccessKeySecret applied in the SMS of Alibaba Cloud.
Confirm AccessKeySecret	Re-type the AccessKeySecret to confirm.
Trading Code	If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the trading code. The range is 1-7.
Channel	If the protocol of SMS gateway that the SP instance is running is XUANWU, you must ask the Xuanwu Technology SMS service platform for the channel. The range is a-z.
Request Type	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the request type. The range is 1-6.
Organization Code	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform

Option	Description
	for the organization code. The range is 1-31.
SMS Service Type	If the protocol of SMS gateway that the SP instance is running is CAS, you can ask the 12302 SMS service platform for the SMS service type. The range is 1-31.
Send Sign Code	When the protocol type is specified as "ACC", select the **Enable** check box to enable the Send Sign Code function. When this function is enabled, the ACC SMS gateway will add a sign code field when sending a request to the ACC server, which will prevent the content of the SMS from being tampered with.

Testing SMS

To test if the message sending works, you can send a test text to a mobile.

To send a text message to a specified mobile number, take the following steps:

1. Select **System > SMS Parameters >SMS Gateway**.
2. Click the "SMS test" link in the **SMS Test** column of the SMS gateway list.
3. In the **Mobile Phone Number** dialog box, enter a mobile phone number in the text box.
4. In the **Test Message Content** dialog box, enter the content of text messages sent to the specified phone number. The default value is "This is a test message, please don't feedback!". Note: If a ChinaMobileMusic service provider name is specified for the "SMS Gateway Name" option, the value range of the content of text messages is 0 to 6 characters.

5. Click **Send**. If the SMS modem is correctly configured and connected, the phone using that number will receive a text message; if it fails, an error message will indicate where the error is.

SMS Parameters

This Section contains the following contents:

- "SMS Modem" on Page 1814
- "SMS Gateway" on Page 1815

VSYS (Virtual System)

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

VSYS (Virtual System) logically divides the physical firewall into several virtual firewalls. Each virtual firewall can work independently as a physical device with its own system resources, and provides most firewall features. A VSYS is separated from other VSYS, and by default, they cannot directly communicate with each other.

VSYS has the following characteristics:

- Each VSYS has its own administrator;
- Each VSYS has an its own virtual router, zone, address book and service book;
- Each VSYS can have its own physical or logical interfaces;
- Each VSYS has its own security policies.



Notes:

- SG-6000-A1100、SG-6000-A1000、SG-6000-A200 and SG-6000-A200W do not support this function.



- The maximum VSYS number is determined by the platform capacity and license. You can expand VSYS maximum number by purchasing addition licenses.

VSYS Objects

This section describes VSYS objects, including root VSYS, non-root VSYS, administrator, VRouter, VSwitch, zone, and interface.

Root VSYS and Non-root VSYS

System contains only one root VSYS which cannot be deleted. You can create or delete non-root VSYSs after installing a VSYS license and rebooting the device. When creating or deleting non-root VSYSs, you must follow the rules listed below:

- When creating or deleting non-root VSYSs through CLI, you must be under the root VSYS configuration mode.
- Only the root VSYS administrators and root VSYS operators can create or delete non-root VSYS. For more information about administrator permissions, see "Device Management" on Page 1690.
- When creating a non-root VSYS, the following corresponding objects will be created simultaneously:
  - A non-root VSYS administrator named admin. The password is vsys_name-admin.
  - A VRouter named vsys_name-vr.
  - A L3 zone named vsys_name-trust.

  For example, when creating the non-root VSYS named vsys1, the following objects will be created:

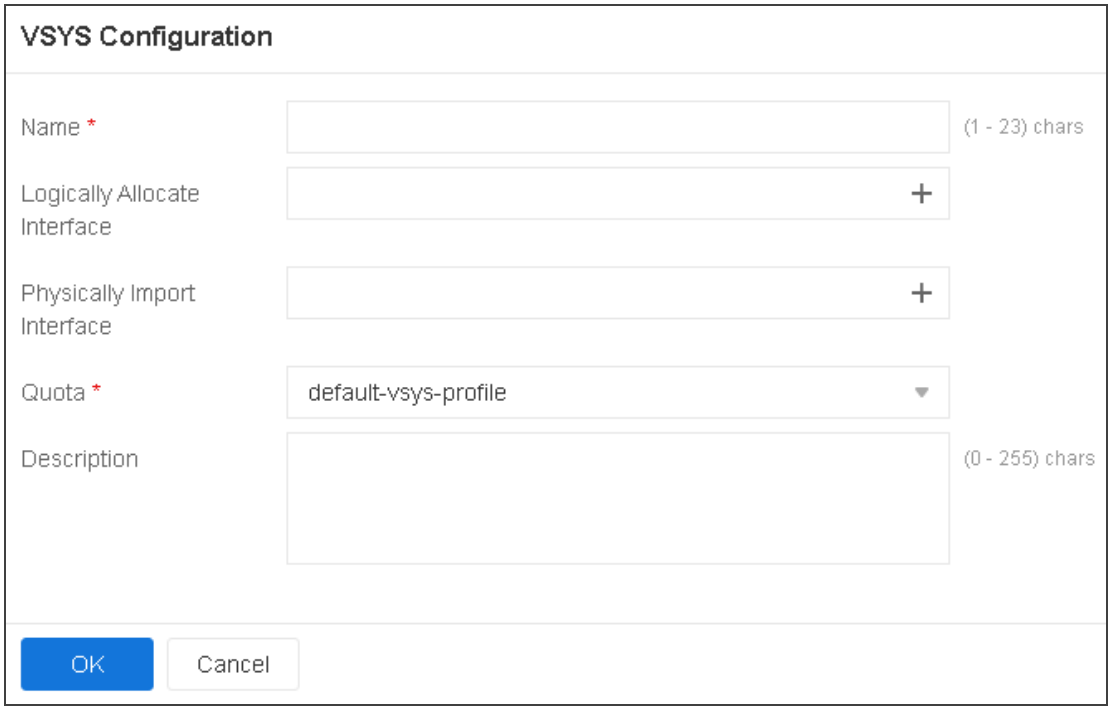
    - The RXW administrator named vsys1\admin with the password vsys1-admin.
    - The default VRouter named vsys1-vr.
    - The L3 zone named vsys1-trust and it is bound to vsys1-vr automatically.
- When deleting a non-root VSYS, all the objects and logs in the VSYS will be deleted simultaneously.
- The root VSYS contains a default VSwitch named VSwitch1, but there is no default VSwitch in a newly created non-root VSYS. Therefore, before creating l2 zones in a non-root VSYS, a VSwitch must be created. The first VSwitch created in a non-root VSYS will be considered as the default VSwitch, and the l2 zone created in the non-root VSYS will be bound to the default VSwitch automatically.

Creating Non-root VSYS

To create a new non-root VSYS, take the following steps:

1. Select **System > VSYS > VSYS**.
2. Click **New** to add a non-root VSYS.

3. In the prompt, configure these values.



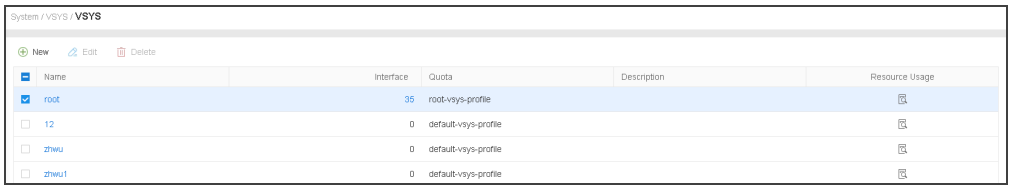
Option	Description
Name	Enter a name for the non-root VSYS.
Description	Enter the description information for the non-root VSYS.
Interface Binding	Select a physical or a logical interface. In VSYS, a physical interface can have its sub-interfaces, but logical interfaces cannot. • Physically Import: Select the interface you want, and click **Physically Import** to add it to the right pane. • Logically Allocate: Select the interface you want, and click **Logically Allocate** to add it to the right pane. • Release: Select the added interface(s), and click **Release** to delete it.

Option	Description
Quota	Select an existing quota.

4. Click **OK** to save configuration. The new VSYS will be seen in the VSYS list.

Viewing VSYS Configuration

The VSYS list displays the configuration of VSYS, including the interface, quota, description, and resource usage. To go to the VSYS page, select **System** > **VSYS** > **VSYS**.



- Click the VSYS name in the **Name** column to go to the WebUI of the VSYS.
- Click the number in the **Interface** column to view the interfaces configured by VSYS.
- Click in the **Resource Usage** column to view the resource usage of VSYS, including the system resources, protection resources, and log configuration resources.

Configuring VSYS Quota

VSYSs work independently in functions but share system resources including concurrent sessions, zone number, policy rule number, SNAT rule number, DNAT rule number, session limit rules number, memory buffer, URL resources, IPS resources, botnet prevention resources, AV resources and PTF resources. You can specify the reserved quota and maximum quota for each type of system resource in a VSYS by creating a VSYS profile. Reserved quota refers to the resource number reserved for the VSYS; maximum quota refers to the maximum resource number available to the VSYS. The root administrator have the permission to create VSYS quota. The total for each resource reserved quota allocated of all VSYSs cannot exceed the system capacity, and the total for each resource actually allocated of all VSYSs cannot exceed the system capacity.

To define a quota for VSYS, take the following steps:

1. Select **System > VSYS > Quota**.
2. Click **New** .
3. In the prompt, configure these values.

Option	Description
Basic Configuration	
Name	Enter a name for the new quota.
CPU	Specify values for parameters of CPU. • Limit: Specifies the maximum performance limit for processing 1 Mbps packets. • Reserve: A dedicated reservered value for CPU in this VSYS. The value range is 0 to 10000. • Alarm Threshold: Specifies a percentage value for alarms. When the CPU usage reaches this value, the system will generate alarm logs.
System Resources	
System Resources	Specify the maximum quota and reserved quota of system resources. • Sessions: Specifies the maximum and reserved number for sessions in the VSYS. • Zone: Specifies the maximum and reserved number for zones in the VSYS. • Policy rules: Specifies the maximum and reserved num-

Option	Description
Basic Configuration	
	ber for policy rules in the VSYS. • Policy Groups: Specifies the maximum and reserved number for policy groups in the VSYS. • SNAT rules: Specifies the maximum and reserved number for SNAT rules in the VSYS. • DNAT rules: Specifies the maximum and reserved number for SNAT rules in the VSYS. • Stat-set (session): Specifies the maximum and reserved number for sessions of a staticstic set in the VSYS. • Stat-set (others): Specifies the maximum and reserved number for other items than sessions of a staticstic set in the VSYS. • IPSec: Specifies the maximum and reserved number for IPSec tunnels in the VSYS. • SSL VPN users: Specifies the maximum and reserved number for SSL VPN users. • Session Limit Rules: Specifies the maximum and reserved number for session limit rules in the VSYS. • Keyword Categories: Specifies the maximum and reserved number for keyword categories in the VSYS. • URL Regex Keywords: Specifies the maximum and

Option	Description
Basic Configuration	
	reserved number for regular expression keywords in a URL category in the VSYS. • Keyword: Specifies the maximum and reserved number for simple keywords in a URL category in the VSYS. • New Session Rate: Specifies the maximum number for the new session rate in the VSYS. • IQoS: Select the **Enable** check box to enable the QoS function and specifies the maximum and reserved number for root-pipe in the VSYS.
Protection	
AV Resources	Specify the maximum quota and reserved quota of AV resources. • AV: Select the **Enable** check box to enable the Anti-Virus function. • AV Profile: Specifies the maximum and reserved number for AV profiles in a VSYS. The range of maximum quota varies from 0 to 32. The reserved quota should not exceed the maximum quota. The default value of maximum quota is 32 and the default value of reserved quota is 0.
URL	Specify the maximum quota and reserved quota of URL

Option	Description
Basic Configuration	
Resources	resources. • URL: Select the **Enable** check box to enable the URL filter function. • URL Profiles: Specifies the maximum and reserved number for URL filter profiles in a VSYS. • URL Categories: Specifies the maximum and reserved number for user-defined URL categories in a VSYS. • URL: Specifies the maximum and reserved number for URLs in a VSYS.
IPS Resources	Specify the maximum quota and reserved quota of IPS resources. • IPS: Select the **Enable** check box to enable the IPS function. • IPS Profiles: Specifies the maximum and reserved number for IPS profiles in a VSYS. You can create up to four IPS profiles in a non-root VSYS. That is, the range of maximum quota is from 0 to 4. The default value is 4. The default value of reserved quota is 0, which means only predefined IPS Profiles can be used in non-root VSYS.
Botnet Prevention	Specify whether to enable the Botnet Prevention function in a VSYS and the maximum quota and reserved quota of botnet pre-

Option	Description
Basic Configuration	
Resources	vention resources. • Botnet Prevention: Select the **Enable** check box to enable the Botnet Prevention function. • In the Profile fields, specify the maximum and reserved number for botnet prevention profiles in a VSYS. The maximum quota ranges from 0 to 32 and the reserved quota cannot exceed the maximum quota. The default values for the maximum quota and the reserved quota are 32 and 0 respectively. **Note**: You can create up to a total of 29 custom botnet prevention profiles in root VSYS and non-root VSYS.
Perimeter Traffic Filtering Resources	Enable or disable perimeter traffic filtering and configure user-defined black/white list resources in a VSYS Profile. • Perimeter Traffic Filtering: Select the **Enable** check box to enable the perimeter traffic filtering function.
Log Configuration	
Log Configuration	Specify the maximum quota and reserved quota of memory buffer for each type of log in a VSYS. The reserved quota should not exceed the maximum quota. If the logs' capacity in a VSYS exceeds its maximum quota, the new logs will override the earliest logs in the buffer.

Option	Description
Basic Configuration	
	• Config Logs: Specify the maximum and reserved value of buffer for configuration logs in a VSYS. • Event Logs: Specify the maximum and reserved value of buffer for event logs in a VSYS. • Network Logs: Specify the maximum and reserved value of buffer for network logs in a VSYS. • Threat Logs: Specify the maximum and reserved value of buffer for threat logs in a VSYS. • Session Logs: Specify the maximum and reserved value of buffer for session logs in a VSYS. • NAT Logs: Specify the maximum and reserved value of buffer for NAT logs in a VSYS. • Web Surfing: Specify the maximum and reserved value of buffer for websurf logs in a VSYS. • PBR: Surfing: Specify the maximum and reserved value of buffer for PBR logs in a VSYS.

4. Click **OK** to save settings. The new VSYS quota will be shown in the list.

Notes:

- Up to 128 VSYS quotas are supported.
- The default VSYS profile of the root VSYS named root-vsys-profile and the default VSYS profile of non-root VSYS named default-vsys-profile cannot be edited or deleted.
- Before deleting a VSYS profile, you must delete all the VSYSs referencing the VSYS profile.
- The maximum quota varies from one platform to another. The reserved quota cannot exceed maximum quota.

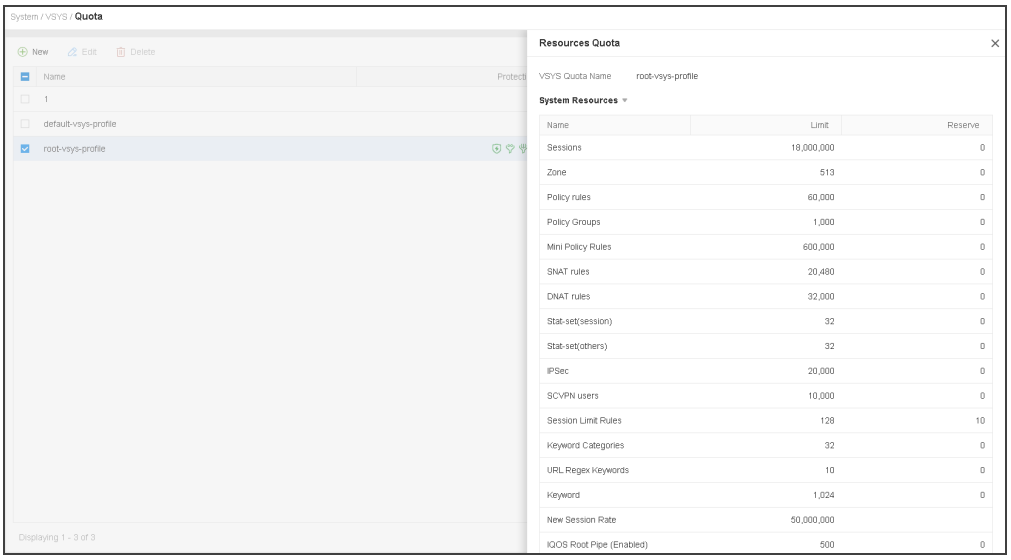
Viewing VSYS Quota

The VSYS quota list displays the resource quota information of VSYS, including the quota name, protection status, and resource quota details.

To view information about the quota of VSYS, take the following steps:

1. Select **System** > **VSYS** > **Quota**.
2. Click in the **Resource Quota** column to view the detailed information about the resource quota of VSYS, including the maximum quota and reserved quota of CPU, system, and log

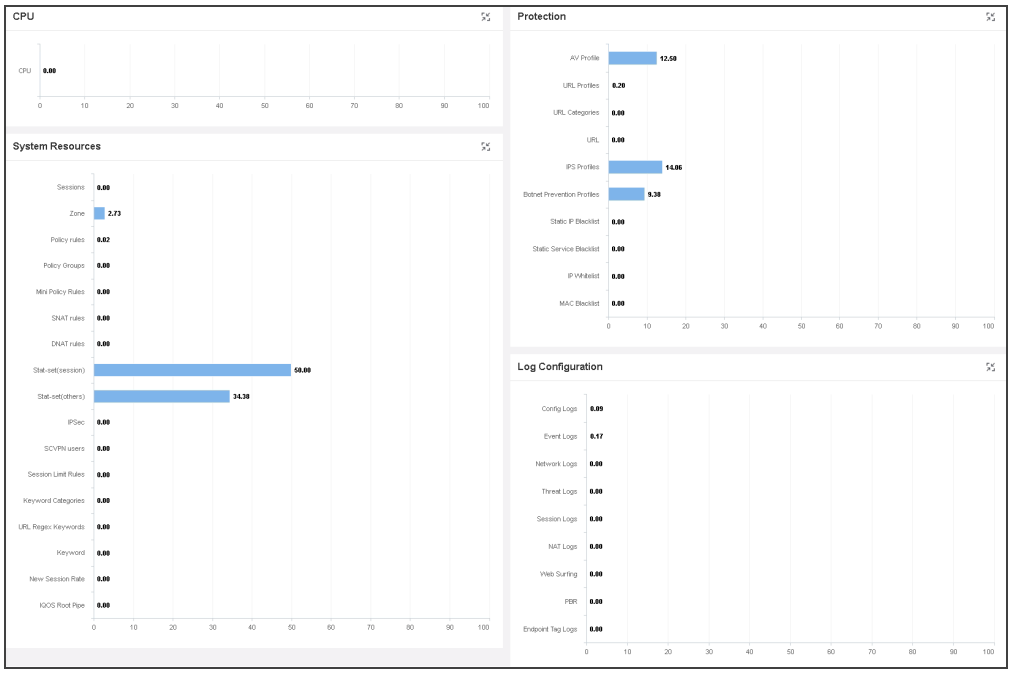
configuration.



Resources

The **Resources** page displays the usage of each resources of VSYS in horizontal bar charts, including the CPU resources, system resources, protection resources, and log configuration resources.

To go to the Resources page, select **System** >**VSYS** > **Resources**.



- Hover your mouse over a horizontal bar chart to view the total number, the number of resources that is used, and the current utilization.
- Click  in the upper-right corner to hide or show the current horizontal bar chart.

Entering the VSYS

To enter a root VSYS, take the following steps:

1. In your browser's address bar, type "https://IP" ("IP" is the management IP of the root VSYS) and press **Enter**.
2. In the login interface, type the username and password, which can be the username and password of the root administrator or the user configured in the authentication server (local server / Radius server / TACACS+ server) of the root VSYS.
3. Click **Login** and enter the root VSYS.

To enter a non-root VSYS, the following two ways are available:

The first way: to enter a non-root VSYS, take the following steps:

1. Enter a root VSYS.
2. In the root VSYS, create a non-root VSYS. For more information on creating non-root VSYS, see **System Management** > **VSYS(Virtual System)** in *StoneOS_WebUI_User_Guide*.
3. In your browser's address bar, type "https://IP" ("IP" is the management IP of the root VSYS) and press **Enter**.
4. In the login interface, type the username (vsys_name\admin) and password (vsys_name-admin) of the non-root administrator. For more information on configuring administrators, see **System Management** > **Device Management** in *StoneOS_WebUI_User_Guide*.
5. Click **Login** and enter the non-root VSYS.

The second way: the root VSYS administrator can enter the non-root VSYS from root VSYS. The administrator in the root VSYS can configure the functions of the non-root VSYS after entering it. To enter a non-root VSYS, take the following steps:

1. Enter a root VSYS.
2. Select **System > VSYS > VSYS** to enter the VSYS page.
3. In the VSYS list, click the name of non-root VSYS, and enter the non-root VSYS.
4. Return to the root VSYS, click  in the right top corner of the page, and click **Return Root VSYS** in the pop-up dialog box.

   Note: If you enter the non-root VSYS directly, you cannot back to the root VSYS.

Logging in to the Device by Using the API Token

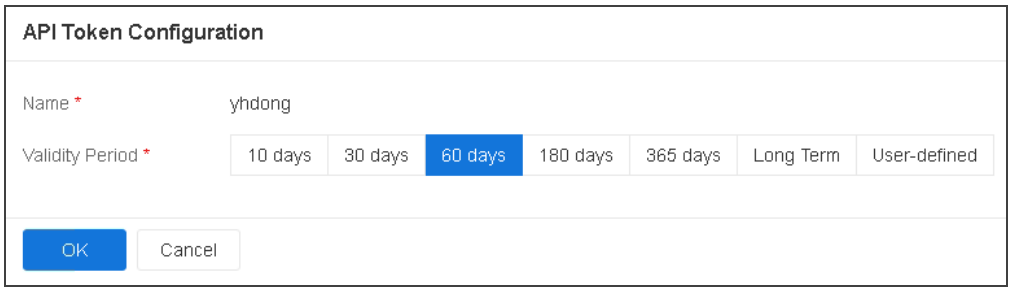
The administrator can use the user name and password or API token authentication when logging in to the device by using RESTful API. You can create an API token for a specified administrator and update, renew, clear, enable, and disable the API token.

Notes: After you enable the SMS or Email authentication, the administrator can only use the API token authentication when logging in to the device by using RESTful API.

Creating an API Token

To create an API token, take the following steps:

1. Select **System** > **Device Management** > **API Token**.
2. Select the administrator that you want to manage and click **Create**.



3. On the API Token Configuration page, configure the following options:

Option	Description
Name	Displays the name of the administrator that wants to create an API token.
Validity Period	Specifies the validity period of the API token. Valid values: 10 days, 30 days, 60 days, 180 days, 365 days, Long Term, and User-defined. Default value: 60 days.

Option	Description
Custom Validity Period	If the Validity Period parameter is set to User-defined, you need to configure this parameter. Valid values: 0 to 365 days.

4. Click **OK**. The newly created API token will be displayed in the API token list and will be enabled by default.

In the API token list, you can also perform the following operations after selecting an API token:

- Click **Update** to update the value of the API token and its validity period. A new API token will be generated after the update.
- Click **Renew** to renew the API token in the enabled or expired state. The value of the API token does not change after the renewal. For example, if the validity period of the administrator "test" is 10 days, the current date November 17, 2022, and the expiration date November 25, 2022, the expiration date will be renewed to November 27, 2022 after the renewal.
- Click **Clear** to delete an API token. If you delete an administrator, the system automatically deletes its API token.
- Click **Enable** to enable an API token. The validity period of the API token will be recalculated. For example, if the original validity period is 30 days, the validity period will become 30 days again after you enable this API token.
- Click **Disable** to disable an API token.
- Click in the **Operation** column to copy the API token, which can be used for RESTful API login.

Secure Connect Client Management

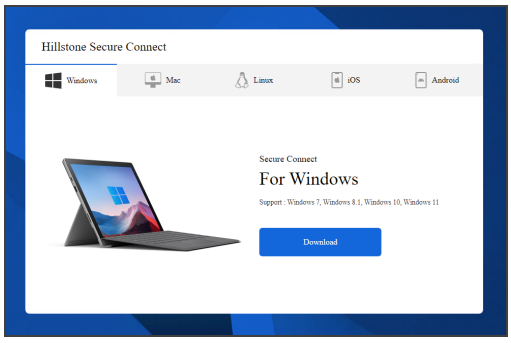
End users can download Secure Connect clients at the following addresses:

- Client download address on the device: https://IP-Address:Port-Number. The "IP-Address" and "Port-Number" refer to the IP address of the egress interface and HTTPS port number specified in the configuration of the SSL VPN or ZTNA instance.
- Client download address provided by Hillstone Networks Official Website https://www.hillstonenet.com/more/services/product-downloads/.

By default, the two addresses use the same download source, and the downloaded Secure Connect client is also the same.

Customizing Secure Connect Download Page

You can customize the title and background of the download address on the device. The default download page is shown as below:



To customize the Secure Connect download page, take the following steps:

1. Select **System > Secure Connect Client Management**.
2. In the "Configure Secure Connect Client Download Page" area, click **Upload Background Picture > Browse** to select the background picture. The picture needs to be PNG format. The recommended resolution is 1920px*1080px. The size cannot exceed 2MB.
3. Click **Upload** to upload the background picture to system. After uploading successfully, you will have completed the background picture modification.

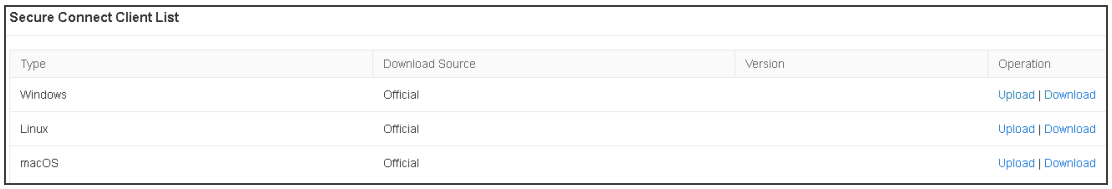
4. Enter the title in the **Download Page Tittle** box to customize the title of the download page. The length is 1 to 63 characters.

5. Click **OK** to save the settings. Clicking **Cancel** will only affect the authentication page title modification.

If you want to restore the default picture, click **Restore Default Background** . Then click **OK**.

Customizing Client Download Source

By default, the client download source on the device is the same with that on Hillstone Networks Official Website. In the application scenario where you want end users to download and use specific Secure Connect clients, such as a client of the specified version or a customized client, you can import the client into the system to overwrite the default download source on the device. You can import Windows, macOS and Linux type clients.



To import the client, take the following steps:

1. Select **System > Secure Connect Client Management**.

2. In the "Secure Connect Client List" area, locate the type of client to be imported and click **Upload**.

3. In the "Upload Secure Connect Client for Windows/macOS/Linux" dialog box, click **Browse** and select the client file to be imported, and click **Upload**. The file name should be in the "xxx_version_check.exe/run/dmg/pkg" format. "xxx" indicates the file name; "version"indicates the client version, starting with the letter "v"; "exe" is the extension for Windows type client file; "run" is the extension for Linux type client file; "dmg" and "pkg" are

the extensions for macOS type client file. The file size cannot exceed 100MB. An example is "secure-connect_v1.4.9.2000_1a6755fe.exe".

4. After uploading, the download source for this client will change from "Offical" to "Local" in the "Secure Connect Client List".
5. Click **Download** to check the downloaded client is the imported one.
6. Click **Delete** to delete the imported client. After the imported client is deleted, the download source will be resorted to "Official".

The Maximum Concurrent Sessions

If multi-VR, AV, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow is enabled on devices, or IPv6 firmware version is used, the maximum concurrent sessions might change. For more information, see the table below:

Platform / Expansion Module	Firmware	Max Concurrent Sessions
SG-6000 A-Series devices	StoneOS IPv4 version	With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the maximum concurrent sessions will not change.
	StoneOS IPv6 version	• The original maximum concurrent sessions of the IPv6 version is the same as that of the IPv4 version; • With multiple virtual routers, anti-virus, IPS, URL signature database, Sandbox, Anti-Spam, Botnet Prevention and/or NetFlow enabled on the system , the maximum concurrent sessions

Platform / Expansion Module	Firmware	Max Concurrent Sessions
		will not change.